Xaica-alpha Security Target Lite

NTTDATA CORPORATION

February 17th, 2005

This document provides summary of Xaica-alpha security features,
based on Xaica-alpha Security Target, NTTD-ST-XAICAALPHA-ST19.

Index

GLOSSARY

Algorithm ID ... Attribute in IEF which means the cryptographic method to be used.

Application Firewall ... Security function to keep out of interfering among applications in multi application smartcard.

Card Issuer ...Administrators of TOE for service which has the responsibility to manage the Card-status, behavior of functions and to give roles to others.

Card manufacturer ... Manufacturing vendor, that has the capability to manufacture smartcards from IC chips and has the responsibility to control the initial state of the TOE in a secure manner when the IC chips are delivered.

Card-status ... Property information which indicates the lifecycle phase of TOE. TOE manages the lifecycle phases as security attribute SA.S_CARDSTATUS.

Certificate verification ... TOE has the function to verify the certificate like X.509. When the certificate is attested as legally the public key in the certificate is temporarily stored on the TOE which is often called TMPKEY.

Chip Configuration ... The lifecycle of ST19XR34. It takes 'ISSUER' , 'TEST' or 'USER'. However, it is fixed as 'USER configuration' after the delivery of TOE from IC chip manufacturer. Therefore , it is always regarded as 'USER configuration' in this security target. It is defined in [ST19XR34-ST].

Composite security function ...Security function on Xaica-PF using security functions provided by dedicated software on ST19XR34

Co-processor ... Processor for arithmetic calculation, especially used for RSA computation

Current position ... Logical location which is determined by 'SELECT' command.

Decryption ... Cryptographic procedure to decode a encrypted message.

Dedicated Software ... Libraries or registers provided for the smartcard platform software programmer by chip manufacturer.

DES ... Data encryption standard. Symmetric cryptography standardized in ISO. TOE supports DES,T-DES2key and T-DES3key.

Downloading ...Function to store files or smartcard applications into TOE.

Encryption ... Cryptographic procedure to scramble a plain message.

Environmental attacks ...It includes High/low voltage attack and High/low frequency attack which may enable the attacker to analyze data inside of smartcard.

(External) command …Communication data sent from external terminal to TOE on Logical interface. All embedded commands are listed in Annex-A.

External terminal … Device or computer PC connected with smartcard reader writer. It can communicate with smartcard via reader writer

File-based application … Smartcard application which consists of RDF, DF, WEF or IEF.

File-ID … Exclusive ID assigned in each objects. ex. RID, AID, DF-name or EFID.

IC chip … Integrated circuit chip on which the smartcard software program runs. Normally it has the physical tampering as security features.

JUKI-network … Japanese residential network service where the smartcard (JUKI-card) is used.

JUKI-card … The smartcard used for JUKI-network which has JUKI-application in it.

JUKI-card issuer … Card issuer in JUKI-service, the local government where the cardholder (resident) live in.

JUKI-application … Smartcard application on the JUKI-card.

Logical interface …Communication interface between smartcard and external terminal defined in ISO7816.

Multi application smartcard … the smartcard which allows coded programs to be downloaded on it.

Physical attack …It indicates the general definition of attacks against smartcard . In this security target it decomposes three types of attacks: (1)Electronic Attacks (2) Environmental Attacks (3) Side Channel Attacks.

Reader writer … Access device for communicating smartcard. **Response** …Communication data sent from TOE to external terminal on logical interface.

Secure messaging … Secure communication protocol between smartcard and external terminal.

Secure messaging key(s) … Keys used for secure messaging**SECURITY ENVIRONMENT (SE)** … Security environment defined in ISO/IEC 7816, which has some security conditions to be managed. **Security status** …Record of successful authentication

SELECT command … Basic command defined in ISO7816-4 for selecting objects in the smartcard.

Self-checking and analysis … TOE self diagnosis function **Smartcard** … A card embedded with IC chip. **Smartcard application** … Set of files or directories downloaded on the smartcard after issue (= File-based application).

Smartcard platform software …The main program which initially starts in the TOE when the TOE is started to run.

Software reset …Same as warm reset defined in ISO/IEC 7816.

ST19XR34 … Product name of IC chip involved in the TOE

STMicroelectronics Corporation …The IC chip manufacturing vendor producing ST19XR34 used in Xaica-alpha

ST-ROM …Exclusive ROM area for STM

T-DES2key … Triple Data encryption standard using two 56-bit keys. Symmetric cryptography standardized in ISO. TOE also supports DES and T-DES2key.

T-DES3key … Triple Data encryption standard using three 56-bit keys. Symmetric cryptography standardized in ISO. TOE also supports DES and T-DES3key.

Test operator … TOE testing operator, one of the development staff.

Timing Attack … Analysis attacks against IC processing, to find confidential information inside of IC by analyzing the time difference of performance.

Temporary public key ... RSA public key temporarily stored on TOE if its signature is certified, like in the method of certificate verification.

Warm reset … It is the function defined in ISO7816 to make TOE reset logically with supplying electric power to the TOE.

Xaica-alpha …Smartcard produced by NTTDATA.

Xaica-PF … Smartcard platform software of Xaica-alpha

Z-application … Embedded financial application on TOE.

ACRONYM

AID … Application ID. Before executing an application on smartcard it must be selected with AID by using SELECT command.

APDU … Application Protocol Data Unit defined in [ISO7816]

CCS … Optional function for secure messaging, which gives the authentication code in the secure messaging APDU for the purpose of ensuring the integrity of APDU

CD … Card domain created by card manufacture in 'init' mode of card-status. Related properties like security attributes or size of domain areas are determined by JUKI-card issuer.

CLA/INS … Class and instruction defined in ISO7816. It is the header of APDU, which indicates some attributes of external command.

DF … Dedicated File (ISO7816)

DFA … Differential fault analysis It is one of the side channel attacks against IC chip which deliberately cause the fault state while IC chip is computing. DFA includes an illegal voltage attacks or electrical noise, and so on.

DPA … Differential power analysis. Attack method to get some power consuming waves and analyze the difference of them in order to know the cryptographic key.

EEPAAB …Access control related security attribute EEPAAB (1byte)..

EEPROM … Non volatile memory on IC chip. Normally it is used for storing data or keys of the smartcard platform or applications, and also often the program application for smartcard is downloaded on it.

EFID … Unique ID assigned in IEF or WEF.

EMA … Electromagnetic analysis

ENC … Optional function for secure messaging which enciphers APDU for the purpose of the confidentiality of APDU.

GUN … The generator of unpredictable number.

HODPA … Higher order differential power analysis

IEF …Internal Elementary File. Normally it is used for storing keys. It has some of the SA.O_* as security attributes.

MAC … Message authentication code. It is used for integrity verification of external command and response in the secure messaging.

MIT/LCS …. MIT/LCS stands for Massachusetts Institute of Technology, Laboratory for Computer Science.

RAM … Volatile memory equipped in the IC chip of smartcard.

R/W… Reader writer.

RDF … Root dedicated file used for file-based application.

RID … It is defined in ISO7816 as code for identifying SD.

ROM … Read only memory equipped in the IC chip of smartcard. Normally it is used for storing the programs of libraries, basic OS, smartcard platform software and embedded applications.

SE … SECURITY ENVIRONMENT.

STM …STMicroelectronics Corporation

SPA … Simple power analysis. It is one of side channel attacks method to analyze the power consuming waves in order to know the cryptographic key.

WEF … Working Elementary File. Normally it is used for storing user data. It has some of the SA.O_* as security attributes.

1. INTRODUCTION

This chapter describes identification of security target (**ST**), the overview of ST, conformance claims, and the structure of this document.

1.1. ST Identification

Title: Xaica-alpha Security Target Lite
Document Identification: NTTD-STL-XAICAALPHA-ST19
Document version: version 1.02
Date: February 17th, 2005
Author: Naohisa ICHIHARA
Company: NTTDATA
Product name: Xaica-alpha
TOE version: VER150i_alpha7rs3_SM032 embedded on ST19XR34F PQB chip

1.2. ST overview

In Japan, smartcards are increasingly implemented for not only financial, transport sectors but also governmental usage. The Japanese residential registry network system (**JUKI-network**) in particular, launched since August 2003, is expected to make smartcard technology come into wide use, that provides residential smartcard (**JUKI-card**). JUKI-card provides **JUKI-service** under JUKI-network for the resident.

This documentation is the security target of **a multi application smartcard** ‘**Xaica-alpha**’ used for JUKI-card provided by **NTTDATA**, compliant with **[JUKI-spec] and [JUKI-type2]** offered by JUKI-network organizer **LASDEC**.

The TOE meets:

ISO7816 for contact interface, some external commands referred to [ISO7816]

ISO14443 type-B for contactless interface, referred to [ISO14443]

JICSAP ver1.1, referred to [JICSAP].

JUKI-specification, referred to [JUKI-network], [JUKI-spec], [JUKI-type2], [JUKI-test].

Xaica-alpha mainly consists of:

- Integrated Circuit Chip for smartcard (ST19XR34) provided by STMicroelectronics (STM)
- Dedicated Software provided in ST19XR34.
- Smartcard platform software 'Xaica-PF' embedded on IC chip
- JUKI-application embedded on Xaica-PF

Note that ST19XR34 has already been certified in the Common Criteria IT security evaluation in October 2004 [CertRepo-ST19XR34].

The main objectives of this security target are:

- To identify the target of evaluation (TOE), the product type, the TOE environment and its lifecycle, and to define the physical and logical boundary of the TOE
- To identify the security environment of the TOE, assets to be protected, envisioned threats to be countered by the TOE and its supporting environment.
- To identify the security objectives for the TOE and for its supporting environment
- To specify the functional security requirements for TOE and IT environment as well as security assurance requirements
- To give the TOE summary specification which explain overview of TOE security functionalities implemented in the product.

Note that any descriptions of rationale are to be removed only in the lite version of security target.

1.3. Common Criteria Conformance Claims

This security target is compliant with the Common Criteria V2.1, part1,2,3.

This security target claims:

- CC V2.1 part2 [CC_part2] extended with
  · "FAU_CFG.1 Configuration management"
- CC V2.1 part3 [CC_part3] as assurance level EAL4 augmented with "AVA_VLA.2 Vulnerability assessment"
- Additionally, ADV_IMP.2 and ALC_DVS.2 are adopted as update of ADV_IMP and ALC_DVS family of EAL4 standard menu.

The minimum strength level for the TOE security function is "SOF-high"

Note that this security target is written with reference to [JUKI-PP].

.

2. TOE DESCRIPTION

This chapter identifies background, product type, the scope and boundary of the TOE.

2.1. Background

This section explains the environmental condition and the intended usage of JUKI-card.

2.1.1. Overview of JUKI-service

JUKI service has the **central server** which manages the database involving residential information. **Local governmental office** has a local server connected with a central server and has **an external terminal** for JUKI-service connected with the local server. The local server and the terminal are used for issuing or providing services, and these are usually operated by public employee in the local government office. The terminal is also connected with **reader writer** for communicating JUKI-card.

A local government issues JUKI-card to resident if he/she needs it. JUKI-card stores information for resident. The resident can receive public services in the local government office with his/her own JUKI-card. Figure 2-1 shows an overview image of JUKI-service.

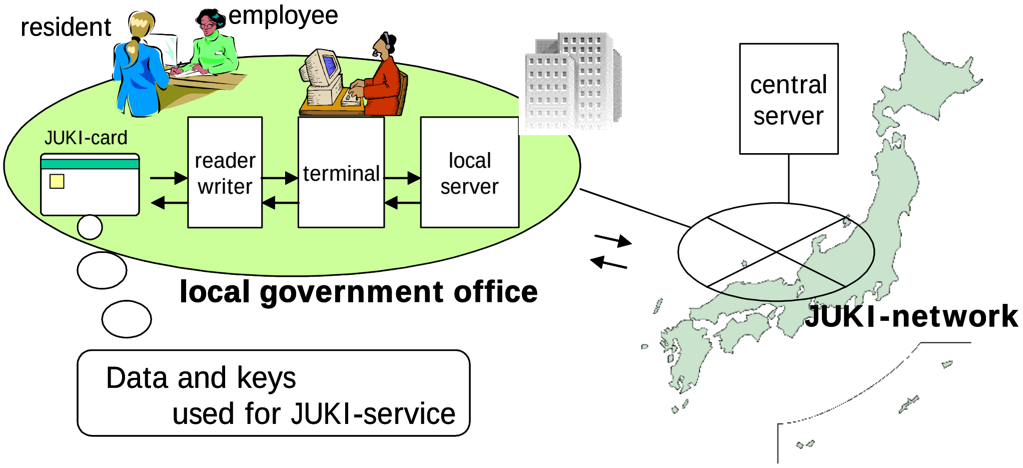

Figure 2-1: Image of JUKI-service

2.1.2. Issuing and personalization

JUKI-card manufactured and issued in smartcard manufacturing factory is delivered to the local government office, and they are stored in the local government office before personalizing.

When the resident requires the local government office to issue JUKI-card, they provide with his/her own JUKI-card with following data and keys:

- Personalized data (**JUKI data**)
- Password determined by the resident (cardholder)
- Some other data and cryptographic keys used for JUKI-service

These procedures are operated by public employee as **personalization operator** in local governmental office.

2.1.3. JUKI-service (intended usage)

JUKI-card is capable of providing JUKI-service for the cardholder if password verification is succeeded by the card holder. JUKI-service is to be operated by public employee as **service operator** in the local governmental office. During JUKI-service processing the communication data between JUKI-card and an external terminal is required to be securely protected from eavesdropping or illegal modification.

2.1.4. Password management

In case that a cardholder of JUKI-card forgets his/her own password, He/she can require the local government to initialize and set the new password. Such a password management service is operated by public employee as a service operator in the local governmental office.

2.1.5. Additional service

The local government might also offer other residential services except JUKI-service. In this case the additional **file-based smartcard application** is to be embedded or downloaded on JUKI-card.

2.2. Product type

Xaica-alpha is a multi-application smartcard used as JUKI-card. Figure 2-2 shows **boundary of the TOE** which includes followings:

- Integrated Circuit Chip for smartcard (ST19XR34) provided by

STMicroelectronics (STM)

- Dedicated Software provided in ST19XR34.
- Smartcard platform software 'Xaica-PF' embedded on IC chip
- JUKI-application embedded on Xaica-PF

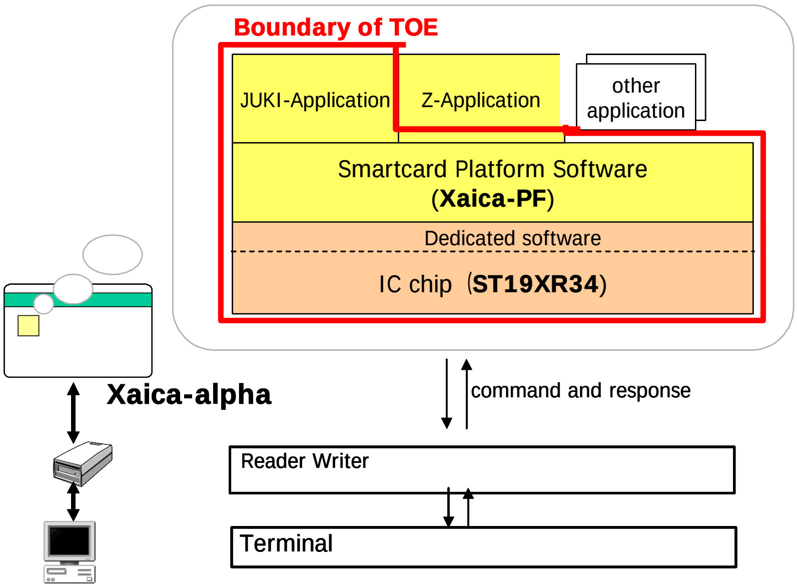

Figure 2-2: TOE boundary

But following is not covered:

- Non metallic parts of card materials
- Surface printings, embossing or magnetic stripes.
- Additional smartcard application downloaded on the TOE

IT security features provided in the TOE are:

- User identification and authentication (security function)
- Access control (security function)
- Cryptography (security function)
- Management of card-status (security function)
- Secure messaging
- Management of secure messaging key
- Management of key and password
- Management of temporary public key
- Download of file-based application
- Management of SECURITY ENVIRONMENT

- Initialization and initial testing (security function)
- Security functions provided in the IC chip
  - Memory partition and access control
  - Cryptographic and random generation libraries
  - Physical tampering and internal integrity

TOE provides some authentication mechanisms to identify the user, and has the access control function in order to avoid any unauthorized user's accessing to the object. TOE always identifies its card-status applicable to lifecycle phase, and restricts the available functions for each card-status. These functionalities are used in the phases from issuing, personalization until JUKI-service.

TOE allows the user to store the key or password as usage, and has stored key management functionality as well. Cryptographic function provided is dedicated not only to cryptographic key and authentication but also secure messaging which ensures the communication data is protected by eavesdropping or illegal modification. These functionalities are required to provide JUKI-service for resident as described above.

In addition, TOE provides the function to check and allow file-based application to be downloaded on the TOE from outside.

Some behavior of above security functions could be managed in SECURITY ENVIRONMENT as defined in [ISO7816].

Xaica-PF and IC chip have and provide the self-management functions so as to keep confidentiality, integrity and availability of TOE functionalities as followings; self-diagnosis, internal integrity checking, physical tampering and detecting, violation administrator, and so on.

2.3. Threat agents

This section identifies attackers to be assumed. This security target requires that measures be taken with respect to the following attackers (unauthorised personnel).

Expert： These are experts with respect to cards who possess specialised knowledge (hardware or software designs, protocols between the card and the reader/ writer, testing/maintenance tools used for testing, algorithm for encryption and digital signature, etc) and who use such specialised knowledge to utilise various devices.

Proficient： People with knowledge of card issuances operations.

Layman： Residents to whom a Residential IC Card is issued, including those who can operate a personal computer and acquire standardised documents.

Those who know the expert or proficient knowledge, are considered as ‘Expert’ or Proficient’.

2.4. Scope of Evaluation

This section identifies the evaluation scopes according to lifecycle phases defined in [PP9806].
This security evaluation scopes from Phase 1 until the end of Phase 3 though only STM is in charge of Phase 2 and 3.

Phase 1: Smartcard embedded software development

NTTDATA and TOPPAN are in charge of the smartcard embedded software of Xaica-alpha development and the specification of IC pre-personalisation requirements.

Phase 2: IC development

STM designs the IC (ST19XR34), develops IC dedicated software, provides information, software or tools to the smartcard embedded software developer, and receives the smartcard embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, he constructs the smartcard IC database, necessary for the IC photomask fabrication.

Phase 3: IC manufacturing and testing

STM is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalisation.

Phase 4: IC packaging and testing

STM is responsible for the IC packaging and testing.

Phase 5: Smartcard product finishing process

Card manufacturer is responsible for the smartcard product finishing process and testing.

Phase 6: Smartcard personalisation

Card issuer (local government in case of JUKI-service) is responsible for the smartcard personalisation and final tests. Other smartcard embedded software may be loaded onto the chip at the personalisation process

Phase 7: Smartcard end-usage

Card issuer (local government in case of JUKI-service) is responsible for the smartcard product delivery to the cardholder, and the end of life process

.

3. TOE security environment

This chapter identifies the following contents:

- **Assets** to be protected by the TOE and/or environment
- **Assumptions** as the intended usage of TOE, possible limitation of use, physical, personnel, or connectivity aspects of
- **Threats** to assets against which specific protection either in the TOE or in its environment is required
- **Organizational security policies** required in JUKI-service to be enforced in the TOE and its environment

3.1. Assets

The Residential IC Card is produced through a variety of manufacturing processes. This security target refers to those data to be protected by the TOE (Target of Evaluation) and to be needed for protections as “primary assets”, and the other data (e.g. documents created in the production processes) as “secondary assets”.

1) Primary assets:

The user data to be protected by the TOE:

- Initialisation data to be set by the local government;
- Card type information to be set by the manufacturer;
- Residents' registration codes to be used by the personal ID application

Moreover, in order to protect these data, the TOE utilizes the following TSF Data (TOE Security Function data such as authentication data and security attributes).

- User authentication data: password, transport keys;
- Terminal authentication data: authentication keys;
- Certificate data: application programs load certificates

In this security target other primary assets are added as described below.

- Smartcard application which can be loaded on the smartcard.
- Memory resources (RAM, ROM, EEPROM and information on the bus)on IC chip

2) Secondary assets：

Information that is produced or used during the manufacturing process of the TOE impacts the integrity or confidentiality of the TOE itself significantly. This kind of information is called ‘ secondary assets’ and the security of such information is established through the diverse assurance requirements that are required by EAL4 , ADV_IMP.2 and ALC_DVS.2. The following is an overview.

ACM Class:

Evidence that unauthorized action has not been taken in the production and manufacturing process with respect to the TOE.

ADO Class:

Evidence that the delivery and installation of the TOE are correctly performed.

ADV Class:

Evidence that the TOE functional requirements have been correctly implemented in the design and development process of the TOE.

AGD Class:

Evidence that the TOE functions and intended usage have been correctly guided.

ALC Class:

Evidence that appropriate security measures have been implemented within the TOE development environment.

ATE Class:

Evidence that the TOE has been appropriately tested.

AVA Class:

Evidence that there is no vulnerability in the TOE.

3.2. Assumptions

This section identifies assumptions including intended usage of TOE and the environmental aspect of TOE usage.

A.TSF_Data :
Throughout the whole life cycle, the TOE is set with various TSF data. Those data should be securely managed at each stage. Moreover, the data goes through IT (Information Technology) devices such as a Reader/Writer or terminal upon setting. Accordingly, those IT devices should be able to manage the TSF data.

3.3. Threats

This chapter identifies presumed threats against which will be required by either TOE or environment.

T.Logical_Attack
The Residential IC Cards delivered to the local government's offices are set with the issuer's initialisation data and resident codes in the memory units and printed with the surface designs. After these issuance processes, the cards are distributed to the residents for use. An attacker with substantial knowledge about IC card technology may make use the logical interfaces (command/response) defined in the Residential IC Card specifications or those proprietarily defined in the relevant card specifications, in order to modify or steal the user data, TSF data

T.Illegal_Term_Use
An attacker who knows the technologies and operations of card terminals under the Residential Information Service Network may use those terminals or modify his/her own personal computers, in order to illegally access the Residential IC Card thus to modify or steal the user data or TSF data.

T.Disturb_APL
There are many applications in a Residential IC Card. That is, the personal ID

application, the proprietary applications loaded by the local government. Inside the card with such multiple applications, the local government's proprietary application may modify or steal the user data (application data of the personal ID).

T.Untrust_Path

An attacker with substantial knowledge on IC card technologies may eavesdrop the user data or TSF data being transmitted between the card and Reader/Writer and analyse the format to estimate the user data or TSF data. If the physical interface is contactless type, the card wirelessly communicates with the Reader/Writer. Therefore, the attacker does not have to tamper with card terminal to eavesdrop the communication data, which will provide an easier environment for the attacker to attack another person's card.

T.Environment

In some cases, the electric power is turned off, or fault injection attacks like DFA might be carried out when a resident is using his/her card and the civil service is thus interrupted. Afterwards, when the service is restarted, the user data or TSF data may be altered or damaged.

T.Incomplete

Prior to the issuance of Residential IC Cards delivered to the local governments' offices, there are various setting processes of data and TSF data. The attacker may illegally use user data or TSF data stored on those cards at the pre-issuance stages, or which are used and tested in the development stage.

T.Hardware

The residential IC card may be attacked from attackers who are well versed in semiconductors or cryptographic technologies.

- by use of FIB (Focused Ion Beam) workstation, EBP (Electron Beam Prober), AFM (Automatic Force Microscope), the attacker physically tampers or eavesdrops (i.e. by tampering the TOE itself or the TSF data, retrieving the TSF data) the processing units or memory elements;
- the attacker estimates the TSF data through the analysis of the hardware processing status;

- the attacker estimates TSF data through the analysis of the results from such card operations in abnormal states.

3.4. Organizational security policies

In this section the related organizational security policies are stated according to [JUKI-network], [JUKI-spec], [JUKI-type2], [JUKI-test].

P.Authentication

“ Residential IC Card Specification Version 2.1” does not define the policies to read out the resident codes. However, the descriptions in Chapter 7 "Residential IC Card Application" Table 8.9 "Security Attribute Settings" implicitly address the following conditions as policies.

- The user authentication should be completed with PIN inputs (SC3).
- The issue authentication should be completed with the certificates issued by the National Residential Information Centre (SC4).

Note) Table 8.9 shows the access privileges. The accesses to the resident codes are subject to the successful PIN-based user authentication (SC3) and to the issuer authentication with certificate National Residential Information Centre (SC4).

P.Secret_Setting

The Business Requirement (1) of Chapter 1 "Overview" Section 2.3 states, "a secure issuance scheme should be adopted for the secret key setting on the card.

P.Card_Activate

The Business Requirement (2) of Chapter 1 "Overview" Section 2.3 states "the card can be used for the residential information services after the resident sets his/her password."

P.PIN_Initialise

The Business Requirement (3) of Chapter 1 "Overview" Section 2.3 states “the card should support the renewal of user’s password after the PIN initialisation for the purpose of reusing when the cardholder forgets his/her own password."

P.Secure_Path

Section 3.4 "Secure Messaging Function" of Chapter 7 "Residential IC Card Application Specifications" states "the secure messaging function should encrypt the APDUs to be transmitted between the card and terminal in order to protect the APDUs from unauthorized eavesdropping. The Residential IC Card application should utilize this function in the process to read out the resident codes.”

Note) APDU (Application Protocol Data Unit) is a unit of data transmitted between the card and Reader/Writer, and this PP refers the APDU transmitted from the Reader/Writer to the card as “command” while the data from card to the Reader/Writer is called “Response”.

4. Security Objectives

This chapter identifies security objectives which address or support TOE security environment aspects identified in the previous chapter. Security objectives are divided into security objectives for the TOE and security objectives for IT environment.

4.1. Security objectives for the TOE

O.Identification

The TSF must provide the mechanism to identify the issuer, resident, terminal and application loaded in the card.

O.Authentication

The TSF must provide the mechanism to limit the accesses from the service program in the terminal to the user data in the TOE to logical interface so that only the Issuers, residents and terminals identified and authenticated by the TOE shall have access to assets.

O.Domain

The TSF must provide the mechanism to limit the accesses from the service program in the terminal to the user data in the TOE to logical interface so that only the Issuers, residents and terminals identified and authenticated by the TOE shall have access to assets.

O.Secure_Path

The TSF must provide the mechanism to prevent the analysis of data format through data communication with the Reader/Writer.

O.Recovery

TSF must have the functionality to recover TSFdata and userdata in the case of unexpected shutdown, as well as to protect, detect and/or recover the assets in the case of fault injection attacks like DFA.

O.Forgery

The TSF must restrict the use of application service without the instruction from an authenticated user by managing the lifecycle status of TOE, in addition the TSF must identify the purpose of TOE usage (TOE mode) as development testing or application service in order to avoid such an illegal operation that the TOE of testing mode is issued in real service.

O.Hardware

TOE must have the capability to resist or detect the electronic, environmental or side channel attacks by an attacker who is well versed in semiconductors or cryptographic technologies. Corresponding attacks are listed below.

1.ELECTRONIC ATTACKS

By use of FIB (Focused Ion Beam) workstation, EBP (Electron Beam Prober), AFM (Automatic Force Microscope), the attacker physically tampers or eavesdrops (i.e. by tampering the TOE itself or the TSF data, retrieving the TSF data) the processing units or memory elements. It also includes:

- Attempts of physically removing the protection shield.

, that is supportive action for electronic attacks

2.ENVIRONMENTAL ATTACKS

The attacker estimates TSF data through the analysis of the results from such card operations in abnormal states. It includes:

- High/low voltage attack
- High/low frequency attack

3.SIDE CHANNEL ATTACKS

The attacker estimates the TSF data through the analysis of the hardware processing status. It includes:

- SPA (Simple power analysis)
- DPA (Differential power analysis)
- EMA (Electromagnetic analysis)
- HO-DPA (Hi-order DPA)
- Timing attack

4.2. Security objectives for environment

This section describes security objectives for environment corresponding to assumptions and/or threats defined above.

OE.TSF_Data

The TSF data that are set in the TOE must be securely managed out of the TOE, in addition, the master key used in real service is stored in the TOE of service usage mode.

OE.Term_TSF

The terminals must securely handle the TSF data used by the Residential IC Card in the authentication process and completely erase the data once the authentication has been completed.

OE.Term_Mgt

The terminals must have the mechanism to prevent any unauthorized use

5. Security functional requirement

This chapter encompasses:

- 5.1 Definitions
- 5.2 TOE security functional requirements
  - 5.2.1 Applicable to TSFs of Xaica-PF
  - 5.2.2 Applicable to composite TSFs of Xaica-PF and ST19XR34
  - 5.2.3 Applicable to TSFs of ST19X34
- 5.3 Dependencies
- 5.4 Minimum strength of function claims

5.1. Definitions

This section defines subjects, objects, roles and security attributes related to TOE security functions controlled under the access control policies. In this security target two different access control mechanisms are defined as they are structured with the hierarchical structure. Access control mechanism in upper layer is provided by Xaica-PF, which works on accessing to data or key from Xaica-PF. The access control mechanism in lower layer is provided by ST19XR34, which works on accessing to memory from any executing process on IC chip. All symbols relating to them are defined in following tables.

Layer	Definition	Table
ST19XR34	Subjects	Table 5-a
	Objects	Table 5-b
	Operations	Table 5-c
	Security attributes	Table 5-d
Xaica-PF	Subjects	Table 5-e
	Objects	Table 5-f
	Operations	Table 5-g
	Security attributes	Table 5-h
	Roles	Table 5-i

5.1.1. ST19XR34 related definitions

Followings are definitions of subjects, objects, operations between them and related security attributes handled in ST19XR34 layer.

Table 5-a: Subjects for ST19XR34

Subjects	Note	Related SFRs
SBJ.STROM_A	SBJ.STROM_A is an executing process of STM's administrative program on ST-ROM..	FPT_TST.1 FDP_ACC.2 FDP_ACF.1[CHIP] FDP_IFF.1[DES] FDP_IFF.1[RSA] FPR_UNO.1
SBJ.LIB_A	STM trusted functional process activated during a call to execute a service available in the STM library.	FDP_ACC.2 FDP_ACF.1[CHIP] FPR_UNO.1
SBJ.ROMA_A	SBJ.ROMA_A is an executing process of smartcard platform software developer's program (Xaica-PF) embedded on ROM-A. I	FDP_ACC.2 FDP_ACF.1[CHIP] FDP_IFF.1[DES] FDP_IFF.1[RSA]
SBJ.EEPROMB_A	SBJ.EEPROMB_A is an executing process of program stored on EEPROM-B.	FDP_ACC.2 FDP_ACF.1[CHIP]
SBJ.EEPROMC_A	SBJ.EEPROMC_A is an executing process of program stored on EEPROM-C.	FDP_ACC.2 FDP_ACF.1[CHIP]

Table 5-b: Objects for ST19XR34

Objects	Note	Related SFRs
OBJ.STROM_A	Data embedded on ST-ROM.	FDP_ACC.2 FDP_ACF.1[CHIP] FPR_UNO.1
OBJ.ROMA_A	Data embedded on ROM-A.	
OBJ.RAMA_A	Data written on RAM-A.	

OBJ.RAMB_A	Data written on RAM-B.	
OBJ.RAMC_A	Data written on RAM-C.	
OBJ.RAMD_A	Data written on RAM-D.	
OBJ.EEPROM_A	Data written on EEPROM-A.	
OBJ.EEPAAB_A	Data written on EEPAAB.	
OBJ.USERREGISTER_A	Register provided for SBJ.ROMA_A	
OBJ.STREGISTER_A	STM's exclusive register provided for SBJ.STROM_A.	

Table 5-c: operations ST19XR34

Operation	Note	Related SFRs
OP.READ_A	Read operation on OBJ.RAM*_A or OBJ.EEPROM_A	FDP_ACC.2 FDP_ACF.1[CHIP] FPR_UNO.1
OP.WRITE_A	Writing '0' or '1' operation on OBJ.RAM*_A	
OP.PROGRAM_A	Operation of writing '1' on OBJ.EEPROM_A	
OP.ERASE_A	Operation of writing '0' on OBJ.EEPROM_A	

Table 5-d: Security attributes ST19XR34

Security attributes	Memo	Related SFRs
SA.LOCATION_A	Dynamic security attributes, which indicates where the current process is executing.	FDP_ACF.1[CHIP] FMT_MSA.3[CHIP]
SA.EEPAAB_A	Access control related security attribute EEPAAB	FDP_ACF.1[CHIP] FMT_MSA.3[CHIP]
SA.INFOTYPE_A	The type of information.	FDP_IFF.1 [DES] FDP_IFF.1 [RSA]

5.1.2. Xaica-PF related definitions

Followings are definitions of subjects, objects, operations between them and related security attributes handled in Xaica-PF layer. However, each subject object is regarded as an instance of subject and object handled on IC chip. Therefore they are managed in both layer's access control mechanism.

Table 5-e: Subjects for Xaica-PF

Subject	Note	Related SFRs
SBJ.XAICAPF	SBJ.XAICAPF is the main executing process embedded on ROM-A, regarded as an instance of SBJ.ROMA_A.	FDP_ACC.1 [JUKI] FDP_ACF.1 [JUKI] FDP_IFF.1 [DES] FDP_IFF.1 [RSA] FPT_TST.1 FAU_SAA.1 FPT_PHP.2

Followings are objects managed in Xaica-PF. OBJ.USD_* means userdata, and OBJ.TSF_* means TSFdata in the definition. All the objects for JUKI-application are created before delivering TOE to the cardholder.

Table 5-f : Objects for Xaica-PF

No	Objects for General	Note	Related SFRs
1	OBJ.USD_WEF	Working Elementary File defined in ISO/IEC 7816.	FDP_ACC.1 [JUKI]
2	OBJ.USD_SCA	Smartcard application	FDP_ITC.1[DLO] FDP_ITC.2[DLO]
3	OBJ.TSF_SMKEY	Secure messaging key stored on RAM	FPT_TDC.1
4	OBJ.TSF_TMPKEY	Temporary public key stored on RAM	FDP_ITC.2[TMPKEY] FIA_UAU.5
5	OBJ.TSF_PIN	PIN stored in IEF used for PIN-verification mechanism	FIA_UAU.5 FIA_AFL.1
6	OBJ.TSF_KEY	Authentication key stored in IEF	FIA_UAU.5

		used for dynamic authentication	FIA_AFL.1
	Objects for JUKI-application	Note	Related SFRs
1	OBJ.USD_WEF_JUKI_INFO1onCD	WEF used in JUKI-application	FDP_ACC.1 [JUKI] FDP_ACF.1[JUKI] FIA_AFL.1 is applied for; OBJ.USD_WEF_JUKI_PUBLICKEYonAP FAU_CFG.1 is applied for; OBJ.USD_WEF_JUKI_INFO*
2	OBJ.USD_WEF_JUKI_INFO2onCD		
3	OBJ.USD_WEF_JUKI_INFO3onCD		
4	OBJ.USD_WEF_JUKI_JDATAonAP		
5	OBJ.USD_WEF_JUKI_INFO2onAP		
6	OBJ.USD_WEF_JUKI_DISTRIBUTE_PKonAP		
7	OBJ.USD_WEF_JUKI_PUBLICKEYonAP		
8	OBJ.TSF_PIN_JUKI_PASSWORDonCD	PIN used in JUKI-application	FIA_UAU.5 FMT_MTD.1 FIA_AFL.1 is applied for OBJ.TSF_IEF_JUKI_PASSWORDonCD
9	OBJ.TSF_PIN_JUKI_PASSWORDonAP		
10	OBJ.TSF_KEY_JUKI_ISSUERPKonCD	Key used in JUKI-application	FIA_AFL.1
11	OBJ.TSF_KEY_JUKI_AUTHORITYPKonAP		

Following operations are performed between subjects and objects managed in Xaica-PF defined above

Table 5-g: Operations for Xaica-PF

Operation	Note	Related SFRs
OP.READ	Read operation on OBJ.USD_WEF*.	FDP_ACC.1 [JUKI] FDP_ACF.1[JUKI]
OP.WRITE	Write operation on OBJ.USD_WEF*.	
OP.SET	Setting operation of OBJ.TSF_SMKEY	
OP.DESTRUCTION	Destruction operation of OBJ.TSF_SMKEY	

Table 5-h: Security attributes for Xaica-PF

Type	Symbol	Note	Related SFRs
Externally specified type (SA.E_*)	SA.E_EXTERNAL	Command Property.	FDP_ACF.1[JUKI]
	SA.E_SIGNATURE	Digital signature associated with SCA or temporary public key.	FDP_ITC.2 [DLO] FDP_ITC.2 [TMPKEY]
Current stated type (SA.C_*)	SA.C_CURRENT	Attributes which are available in the current session	FDP_ACF.1[JUKI] FIA_UAU.1
Status type (SA.S_*)	SA.S_MODE	TOE mode	FDP_ACF.1[JUKI] FIA_UID.1 FMT_MSA.1[MODE] FMT_MSA.3[MODE]
	SA.S_CARDSTATUS	Card-status. Its value takes *'initial'*, *'manufacturing'*, *'pre-production'*, *'initialization'*, *'password-setting'*, *'CD-Secured'*, *'CD-locked'* or *'CD-Terminated'*	FDP_ACF.1[JUKI] FDP_ACF.1[CHIP] FMT_MTD.1
	SA.S_STATUS	Status of SD, RDF, DF, IEF. Value takes *'normal'* or *'locked'*	FDP_ACF.1[JUKI]
Object property type	SA.O_ACCESS	Security attributes for access right associated with SD,AP, RDF, DF, IEF or WEF.	FDP_ACF.1[JUKI] FMT_MSA.1[JUKI]

	SA.O_KEYID	Key ID	FIA_ATD.1 FMT_MSA.1[JUKI]

Table 5-i : Roles for Xaica-PF

Role	Note	Related SFRs
ROL.CARDMAN	Card manufacturer	FIA_UAU.5 FDP_ACF.1[JUKI] FMT_MOF.1 [JUKI] FMT_MTD.1 FMT_SMR.1 FMT_MSA.1[CHIP] FMT_MSA.3[CHIP] FMT_MSA.3[MODE]
ROL.ISSUER1	Issuer1	FIA_UAU.5 FMT_MOF.1 [JUKI] FMT_SMR.1 FMT_MSA.1[CHIP] FMT_MSA.3[CHIP]
ROL.ISSUER2	Issuer2	FIA_UAU.5 FDP_ACF.1[JUKI] FMT_MOF.1 [JUKI] FMT_MSA.1[JUKI] FMT_MSA.3[JUKI] FMT_MTD.1 FMT_SMR.1
ROL.JLOCALGOV	Local government	FIA_UAU.5 FMT_MOF.1 [JUKI] FMT_MTD.1 FMT_SMR.1
ROL.JOPERATOR	JUKI service operator	FIA_UAU.5 FMT_MOF.1 [JUKI] FMT_SMR.1 FMT_MTD.1

ROL.JCARDHOLDER	JUKI card holder	FIA_UAU.5 FMT_MOF.1 [JUKI] FMT_SMR.1 FMT_MTD.1
ROL.TEST	ES developer	FIA_UAU.5 FMT_SMR.1
ROL.TRUST	Any trusted role, defined after issue	FDP_ACF.1[JUKI] FMT_MOF.1 [SE] FMT_SMR.1

5.1.3. Hierarchical access control policy

This subsection describes the overview of the concept of access control polices stated in this security target. TOE has the 'hierarchical' access control mechanism. SFP.CHIP mainly enforces on the access controls between executing process and memory resources enforced by ST19XR34. SFP.ACCESS contributes to the access controls between process and Userdata or TSFdata stored on EEPROM for Xaica-PF. SFP.ACCESS is enforced by Xaica-PF.

5.1.4. Access control policy for IT environment

Hereby, the access control policy for IT environment SFP.ENV is defined.

5.1.5. Information flow control policy

Information flow control policies are dedicated to the confidentiality or integrity of data or keys for cryptographic functions, which are defined as SFP.DES and SFP.RSA.

5.1.6. Key erasing method

Xaica-PF has two methods for key erasing;
MET.ERASE_SMKEY and MET.ERASE_TMPKEY

5.1.7. Key distribution method for secure messaging

Before secure messaging is established the secure messaging key must be shared between external terminal and TOE, the methods of which are;
MET.SET_SESSION_KEY,
MET.GET_SESSION_KEY
MET.DISTRIBUTE_SESSION_KEY
MET.CHECK_SESSION_KEY

5.1.8. Key distribution method for temporary public key

When RSA public key is temporarily stored on TOE, its signature must be verified. The methods of key distribution is,
MET.VERIFY_CERTIFICATE, MET.SET_PUBLIC_KEY

5.1.9. Authenticated status

SC1, SC2, SC3 and SC4 are the status of authentication.

5.2. TOE Security functional requirements

This section described TOE security functional requirements. Some of them are quoted from [ST-ST19XR34] and the rest is originally added in this security target.

- Subsection 5.2.1 defines security requirements applicable to security functions of Xaica-PF only.
- Subsection 5.2.2 defines composite security requirements applicable to both security functions of Xaica-PF and ST19XR34.
- Subsection 5.2.3 defines security requirements applicable to security functions of ST19XR34 only.

There is one explicitly stated TOE security functional requirement as FAU_CFG.1.

5.2.1. Applicable to TSFs of Xaica-PF

(1). FAU_CFG.1 Configuration generation

FAU_CFG.1.1 The TSF shall maintain the configuration file as an object.

FAU_CFG.1.2 The TSF shall record within the configuration file at least the following configuration data

1) Classification ID of smartcard

2) Issuing ID, Local Government ID stored on OBJ.USD_WEF_JUKI_INFO*

Dependencies: No dependency

Application note:

FAU_CFG.1 is explicitly stated as one additional security requirement in this security target.

(2). FCS_CKM.1 [SMKEY] Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with random number generation and specified cryptographic key sizes of 118, 128, 172, 192, 256 bits that meet the following standards: NIST FIPS PUB-140-2:1999 for a security level 3 cryptographic module (statistical test on demand) when the key distribution method MET.GET_SESSION_KEY is used.

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

(3). FCS_CKM.1 [RSAKEY] Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA key pair generation and specified cryptographic key sizes of 1024, 2048 bits that meet the following: private key and public key defined in PKCS#1.

Dependencies: [FCS_CKM.2 Cryptographic key distribution
or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

(4). FCS_CKM.2 [SMKEY] Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method :

- MET.SET_SESSION_KEY,
- MET.GET_SESSION_KEY,
- MET.DISTRIBUTE_SESSION_KEY,
- MET.CHECK_SESSION_KEY

that meets the following: Xaica-alpha secure messaging key distribution.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

(5). FCS_CKM.2 [TMPKEY] Cryptographic key distribution

Hierarchical to: No other components.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method:

- MET.VERIFY_CERTIFICATE,
- MET.SET_PUBLIC_KEY

that meets the following: Xaica-alpha temporary public key distribution.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

(6). FCS_CKM.4 [SMKEY] Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method MET.ERASE_SMKEY that meets the following: none.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

(7). FCS_CKM.4 [TMPKEY] Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method MET.ERASE_TMPKEY that meets the following: none.

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

(8). FDP_ACC.1 [JUKI] Subset access control

Hierarchical to: No other components.

FDP_ACC.1 [JUKI].1 The TSF shall enforce SFP.ACCESS on following listed subjects and objects and following operations among subjects and objects covered by the SFP.ACCESS.

Table 5-j: Subjects and Objects for access control

Item	Purpose	Name
Subjects	For General	SBJ.XAICAPF
Objects	For General	OBJ.USD_WEF
		OBJ.TSF_SMKEY
	For JUKI -application	OBJ.USD_WEF_JUKI_INFO1onCD
		OBJ.USD_WEF_JUKI_INFO2onCD
		OBJ.USD_WEF_JUKI_INFO3onCD
		OBJ.USD_WEF_JUKI_JDATAonAP
		OBJ.USD_WEF_JUKI_INFO2onAP
		OBJ.USD_WEF_JUKI_DISTRIBUTE_PKonAP
		OBJ.USD_WEF_JUKI_PUBLICKEYonAP

Table 5-k : Operations between subjects and objects

Operations		Subjects
		SBJ.XAICAPF
Objects	OBJ.USD_WEF*	OP.READ OP.WRITE
	OBJ.TSF_SMKEY	OP.SET OP.DESTRUCTION

Dependencies: FDP_ACF.1 Security attribute based access control

Application note: OBJ.TSF_SMKEY is regarded as userdata before it is successfully imported on the TOE. After imported, it is regarded as TSFdata before it is destructed.

(9). FDP_ACF.1 [JUKI] Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce SFP.ACCESS to objects based on following security attributes.

Table 5-l: Security attributes for SFP.ACCESS

Externally specified security attributes	Current stated security attributes
SA.E_EXTERNAL	SA.C_CURRENT
Status type of security attributes	**Object property type of security attribute**
SA.S_MODE SA.S_CARDSTATUS SA.S_STATUS	SA.O_ACCESS

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed according to following rules:

[FDP_ACF.1.1_Rule_1] (JUKI-service)

SBJ.XAICAPF can perform following operations against corresponding objects as shown in below if the condition AST.* is satisfied. AST.* means the condition of security attribute SA.C_CURRENT described in section 5.1.

Table 5-m: Access rules for JUKI-service enforced by SBJ.XAICAPF

<< The table is removed >>

[FDP_ACF.1.1_Rule_2] (General)

Subject is allowed to perform operation accessing to OBJ.USD_WEF* only if SA.E_EXTERNAL, SA.S_CARDSTATUS (and SA.S_STATUS) meet SA.C_CURRENT referring to following table. Additionally, in case of ‘T’, SA.C_CURRENT must satisfy SA.O_ACCESS of OBJ.USD_WEF*.

Table 5-n: Rules for accessing to OBJ.USD_WEF*

<< The table is removed >>

[FDP_ACF.1.1_Rule_3] (Secure messaging key setting and distribution)

OP.SET on OBJ.TSF_SMKEY is allowed when it is imported to the TOE in a specified manner that enforces [FDP_ITC.1.3_SMKEY_Rule_1]

[FDP_ACF.1.1_Rule_4] (Secure messaging key destruction)

OP.DESTRUCTION on OBJ.TSF_SMKEY is allowed when it is shared between TOE and remote IT product, which achieves in accordance with a specified key destruction method MET.ERASE_SMKEY.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules.

[FDP_ACF.1.4_Rule_1] (Other subject)

TSF denies any operations against OBJ.USD_WEF* by any other subject except SBJ.XAICAPF.

[FDP_ACF.1.4_Rule_2] (Terminated)

TSF denies any subject's accessing to the object if SA.S_CARDSTATUS indicates 'CD-terminated'.

[FDP_ACF.1.4_Rule_3] (Access rejects)

TSF denies any subject's accessing to the object if SA.O_ACCESS indicates 'forbidden' regarding required operation.

Dependencies: FDP_ACC.1 [JUKI] Subset access control,
FMT_MSA.3 Static attribute initialisation

(10). FDP_ITC.1 [DLO] Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the SFP.ACCESS when importing OBJ.USD_SCA , controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with OBJ.USD_SCA when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing OBJ.USD_SCA controlled under the SFP from outside the TSC:

[FDP_ITC.1.3_DLO_Rule_1]
TSF allows OBJ.USD_SCA without verification of signature only if SA.O_ACCESS of current directory indicates 'no need of signature'.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

(11). FDP_ITC.1 [JUKI] Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the SFP.ACCESS when importing OBJ.TSF_KEY* or OBJ.TSF_PIN*, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with OBJ.TSF_KEY* or OBJ.TSF_PIN* when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: none.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

(12). FDP_ITC.1 [SMKEY] Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the SFP.ACCESS when importing OBJ.TSF_SMKEY, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with OBJ.TSF_SMKEY when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing OBJ.TSF_SMKEY controlled under the SFP from outside the TSC:

[FDP_ITC.1.3_SMKEY_Rule_1]
SF_SMKEY performs following secure messaging key distribution method corresponding to the received command.

Received command	Key distribution method
CHECK_SESSION_KEY	MET.CHECK_SESSION_KEY
GET_SESSION_KEY	MET.GET_SESSION_KEY
SET_SESSION_KEY	MET.SET_SESSION_KEY
DISTRIBUTE_SESSION_KEY	MET.DISTRIBUTE_SESSION_KEY

Dependencies: [FDP_ACC.1 [JUKI] Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

(13). FDP_ITC.2 [DLO] Import of user data with security attributes

Hierarchical to: No other components.

FDP_ITC.2.1 The TSF shall enforce the SFP.ACCESS when importing OBJ.USD_SCA, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes SA.E_SIGNATURE associated with the imported OBJ.USD_SCA .

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes SA.E_SIGNATURE of the imported OBJ.USD_SCA is as intended by the source of the OBJ.USD_SCA.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing OBJ.USD_SCA controlled under the SFP.ACCESS from outside the TSC:

[FDP_ITC.2.5_DLO_Rule_1]
TSF verifies SA.E_SIGNATURE with OBJ.USD_SCA to ensure that SA.E_SIGNATURE is made from OBJ.USD_SCA in RSA signature format.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

(14). FDP_ITC.2 [TMPKEY] Import of user data with security attributes

Hierarchical to: No other components.

FDP_ITC.2.1 The TSF shall enforce the SFP.ACCESS when importing OBJ.TSF_TMPKEY, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes SA.E_SIGNATURE associated with the imported OBJ.TSF_TMPKEY.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes SA.E_SIGNATURE of the imported OBJ.TSF_TMPKEY is as intended by the source of the OBJ.TSF_TMPKEY .

FDP_ITC.2.5 The TSF shall enforce the following rules when importing OBJ.TSF_TMPKEY controlled under the SFP.ACCESS from outside the TSC:

[FDP_ITC.2.5_TMPKEY_Rule_1]
TSF verifies SA.E_SIGNATURE with OBJ.TSF_TMPKEY to ensure that SA.E_SIGNATURE is made from OBJ.TSF_TMPKEY with RSA signature mechanism.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

(15). FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when following unsuccessful authentication attempts occur related to authentication using following keys

Table 5-o: limit of unsuccessful authentication

Limit	List of authentication events	Related key or PIN
1 to 15 (*)	VERIFY EXTERNAL AUTHRNTICATE VERIFY DIGITAL SIGNATURE	OBJ.TSF_PIN* OBJ.TSF_KEY* except below
3	VERIFY	OBJ.TSF_PIN_JUKI_PASSWORDonCD
3	EXTERNAL AUTHRNTICATE	OBJ.TSF_KEY_JUKI_ISSUERPKonCD
3	EXTERNAL AUTHRNTICATE	OBJ.TSF_ IEF_JUKI_AUTHORITYPKonAP
3	VERIFY	OBJ.TSF_PIN_JUKI_PASSWORDonAP

(*)limit number is determined when the key or PIN is created.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall lock the key or PIN

Dependencies: FIA_UAU.1 Timing of authentication

Application note:

Once the key is locked it can not be used for authentication or computation until it is unlocked by authorized user. Unlock function is related to FTM_MOF.1[JUKI].

(16). FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following security attributes belonging to individual users:

- Key ID (SA.O_KEYID) for user identification
- AID for application identification

Dependencies: No dependencies

(17). FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow following TSF mediated actions on behalf of the user to be performed before the user is authenticated.

Table 5-p: TSF mediated actions

Card-status (SA.S_CARDSTATUS) in case SA.S_MODE is 'normal'	TSF mediated actions (External command)
Initial	GET STATUS, GET CHALLENGE VERIFY ROM KEY
Manufacturing Pre-production Password-setting	GET STATUS, GET CHALLENGE VERIFY ROM KEY, SELECT FILE VERIFY, EXTERNAL AUTHENTICATE
Initialization CD-secured	GET STATUS GET CHALLENGE SELECT FILE VERIFY EXTERNAL AUTHENTICATE SELECT WITH AUTHENTICATE GET DEFAULT AP
CD-locked	GET STATUS, GET CHALLENGE, SELECT FILE ,VERIFY, EXTERNAL AUTHENTICATE GET DEFAULT AP
CD-Terminated	None

In addition, GET CHALLENGE and VERIFY ROM KEY is always available as TSF-mediated actions if and only if SA.S_MODE is 'test'

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

(18). FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to

- Dynamic authentication mechanism
- Dynamic authentication mechanism after certificate verification

Dependencies: No dependencies

(19). FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide following authentication mechanisms to support user authentication.

Table 5-q: Multiple authentication mechanism

Authentication mechanism	Type of key	Related roles
PIN-verification	OBJ.TSF_PIN*	ROL.ISSUER1 ROL.ISSUER2 ROL.JOPERATOR, ROL.JCARDHOLDER
Dynamic authentication	OBJ.TSF_KEY*	ROL.JLOCALGOV ROL.CARDMAN, ROL.TEST
Static authentication	OBJ.TSF_KEY*	
Dynamic authentication with temporary public key	OBJ.TSF_TMPKEY	
Static authentication with temporary public key	OBJ.TSF_TMPKEY	

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the following rules.

[FIA_UAU.5.2_Rule_1]

'PIN-verification' with OBJ.TSF_PIN*requires user to set password to be compared with stored PIN.

[FIA_UAU.5.2_Rule_2]

'Dynamic authentication' or 'Dynamic/static authentication with temporary public key' requires user to use random number generated by TOE as a plain message to be signed.

[FIA_UAU.5.2_Rule_3]

‘Static authentication’ or ‘Static authentication’ with temporary public key’ does not require user to use specified plain message to be signed.

Dependencies: No dependencies

(20). FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the following conditions.

[FIA_UAU.6.1_Condition_1]

If Power-on or warm reset is performed, TSF shall clear all records of SA.C_CURRENT. Then TSF requires re-authentication to any user authorized just before.

[FIA_UAU.6.1_Condition_2]

If the user failed to authenticate him again, TSF shall clear the user's record from SA.C_CURRENT. Then TSF requires re-authentication to the user.

[FIA_UAU.6.1_Condition_3]

If the current directory position of SA.C_CURRENT is moves, TSF determines if the user's record of SA.C_CURRENT must be clear according to SA.O_ACCESS. If cleared. TSF requires re-authentication to the user.

Dependencies: No dependencies

(21). FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow following TSF-mediated actions on behalf of the user to be performed before the user is identified.

Table 5-r: TSF-mediated actions

Card-status (SA.S_CARDSTATUS) in case SA.S_MODE is 'normal'	TSF mediated actions (External command)
Initial	GET STATUS, GET CHALLENGE VERIFY ROM KEY
Manufacturing Pre-production Password-setting	GET STATUS, GET CHALLENGE VERIFY ROM KEY, SELECT FILE VERIFY, EXTERNAL AUTHENTICATE
Initialization CD-secured	GET STATUS GET CHALLENGE SELECT FILE VERIFY EXTERNAL AUTHENTICATE SELECT WITH AUTHENTICATE GET DEFAULT AP
CD-locked	GET STATUS, GET CHALLENGE, SELECT FILE ,VERIFY, EXTERNAL AUTHENTICATE GET DEFAULT AP
CD-Terminated	None

In addition, GET CHALLENGE and VERIFY ROM KEY is always available as TSF-mediated actions if and only if SA.S_MODE is 'test'

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

(22). FMT_MOF.1 [JUKI] Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of following functions to authorized identified roles listed below.

<< The table is removed >>

Dependencies: FMT_SMR.1 Security roles

(23). FMT_MOF.1 [SE] Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of following functions to ROL.TRUST by managing SECURITY ENVIRONMENT (ISO/IEC7816).

Security functions
Certificate verification
Signature verification
Signature computation
Secure messaging key distribution
Secure messaging

Dependencies: FMT_SMR.1 Security roles

(24). FMT_MSA.1 [JUKI] Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the SFP.ACCESS to restrict the ability to change_default the security attributes SA.O_* associated with OBJ.TSF_KEY* or OBJ.TSF_PIN* to ROL.ISSUER2.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control or
FDP_IFC.1 Subset information flow control],
FMT_SMR.1 Security roles

(25). FMT_MSA.1 [MODE] Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the SFP.ACCESS to restrict the ability to change_default the security attributes SA.S_MODE to ROL.CARDMAN.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control or
FDP_IFC.1 Subset information flow control],
FMT_SMR.1 Security roles

(26). FMT_MSA.3 [JUKI] Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the SFP.ACCESS to provide restrictive default values for security attributes SA.O_* that are used to enforce the SFP.ACCESS.

FMT_MSA.3.2 The TSF shall allow the ROL.ISSUER2 to specify alternative initial values to override the default values when OBJ.TSF_KEY* or OBJ.TSF_PIN* are created.

Dependencies: FMT_MSA.1 Management of security attributes,
FMT_SMR.1 Security roles

(27). FMT_MSA.3 [MODE] Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the SFP.ACCESS to provide restrictive default values 'normal' for security attributes SA.S_MODE that are used to enforce the SFP.ACCESS.

FMT_MSA.3.2 The TSF shall allow the ROL.CARDMAN to specify alternative initial values to override the default values when 'system track' is created.

Dependencies: FMT_MSA.1 Management of security attributes,
FMT_SMR.1 Security roles

(28). FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to change_default or modify the OBJ.TSF_PIN_JUKI_PASSWORD* to ROL.ISSUER2, ROL.JOPERATOR, ROL.JLOCALGOV, ROL.JCARDHOLDER

<< The table is removed >>

Dependencies: **FMT_SMR.1 Security roles**

(29). FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain following roles.

ROL.CARDMAN

ROL.ISSUER1

ROL.ISSUER2

ROL.JLOCALGOV

ROL.JOPERATOR

ROL.JCARDHOLDER

ROL.TRUST

ROL.TEST

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

(30). FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

(31). FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit TSF to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for read operation on OBJ.USD_WEF_JUKI_JDATAonAP.

Dependencies: No dependencies

Application note:
According to P.Secure_Path, OBJ.USD_WEF_JUKI_JDATAonAP must be read with secure messaging.

(32). FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret OBJ.TSF_SMKEY when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [FDP_ITC.1.3_SMKEY_Rule_1] when interpreting the TSF data from another trusted IT product.

Dependencies: No dependencies

5.2.2. Applicable to composite TSFs of Xaica-PF and ST19XR34

(33). FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform in accordance with following specified cryptographic algorithm and following specified cryptographic key sizes that meet the following standards as specified below.

Table 5-s: Cryptographic algorithms and features

Algorithm	Cryptographic operations	Key size	Standard
T-DES	Encryption and decryption in Cipher Block Chaining (CBC) mode and compute a Message Authentication Code (MAC)	112 or 168	ISO 8372:1987, ISO 8731-1:1987, ISO/IEC 9797:1994 ISO/IEC 10116:1997
RSA	Signature (decryption) Recovery (encryption)	1024, 2048 bits	ISO/IEC 9796-2:1997 and MIT/LCS/TR-212.
RSA_CRT	Signature (decryption)	Same as above	
SHA1	Secure hash function	Result size of 160 bits on chained blocks of 512 bits	NIST FIPS 180-1:1995 and ISO/IEC 10118-3:1998

Dependencies: [FDP_ITC.1 Import of user data without security attributes
or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

(34). FDP_IFC.1 [DES] Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the SFP.DES on

Subject: SBJ.XAICAPF

Information : message, key

Operation : load, unload

Dependencies: FDP_IFF.1 Simple security attributes

(35). FDP_IFC.1 [RSA] Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the SFP.RSA on

Subject: SBJ.XAICAPF

Information : message, key

Operation : load, unload

Dependencies: FDP_IFF.1 Simple security attributes

(36). FDP_IFF.1 [DES] Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the SFP.DES based on the following types of subject and information security attributes:

- the type of information (SA.INFOTYPE_A)

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[FDP_IFF.1.2_DES_Rule_1]:

TSF allows subject to use operation on condition described as below.

Table 5-t: Rules for information flow of DES

	SA.INFOTYPE_A	
	'Message'	*'Key'*
SBJ.ROMA_A	Permit	Permit
	Operation: Load	Operation: Load
	Operation: Unload	Operation: Load
Other subjects	Forbidden	Forbidden

FDP_IFF.1.3 The TSF shall enforce no additional information flow control SFP rules

FDP_IFF.1.4 The TSF shall provide the following : no additional SFP capabilities.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: none.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: none.

Dependencies: FDP_IFC.1 Subset information flow control,

FMT_MSA.3 Static attribute initialisation

(37). FDP_IFF.1 [RSA] Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1 The TSF shall enforce the SFP.RSA based on the following types of subject and information security attributes:.

- the type of information (SA.INFOTYPE_A)

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[FDP_IFF.1.2_RSA_Rule_1]:

TSF enforces the following rules.

Table 5-u :Rules for information flow of RSA

	SA.INFOTYPE_A	
	'Message'	*'Key'*
SBJ.ROMA_A	Permit - Load Operation for RSA, RSA_CRT - Unload Operation for RSA, RSA_CRT	Permit - Load Operation for RSA, RSA_CRT
Other subjects	Forbidden	Forbidden

FDP_IFF.1.3 The TSF shall enforce no additional information flow control SFP rules

FDP_IFF.1.4 The TSF shall provide the following: no additional SFP capabilities.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: none

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: none].

Dependencies: FDP_IFC.1 Subset information flow control,

FMT_MSA.3 Static attribute initialisation

(38). FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet NIST FIPS PUB-140-2:1999 standard for a Security Level 3 cryptographic module (statistical test upon demand)

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for the key distribution method MET.GET_SESSION_KEY provided.

Dependencies: No dependencies

(39). FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- Downloading discontinuity by unexpected shutdown or illegal procedures
- A single bit failure while writing data on EEPROM by unexpected shutdown
- All bits are set to one in a byte and its redundancy data upon a read operation
- Two bits fails on a read operation on each byte

Dependencies: ADV_SPM.1 Informal TOE security policy model

(40). FPT_RCV.2 Automated recovery

Hierarchical to: FPT_RCV.1

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For

- A single bit error while writing data on EEPROM by unexpected shutdown
- A smartcard application downloading discontinuity by unexpected shutdown or bad sequence

, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

Dependencies: FPT_TST.1 TSF testing,
AGD_ADM.1 Administrator guidance,
ADV_SPM.1 Informal TOE security policy model

(41). FPT_RCV.4 Function recovery

Hierarchical to: No other components.

FPT_RCV.4.1 The TSF shall ensure that following SFs and failure scenarios

Table 5-v: Failure scenarios

No.	SFs	Failure scenarios
1	SF_INT_A	a single bit error while writing data on EEPROM by unexpected shutdown
2	SF_DOWNLOAD	a Smartcard application downloading discontinuity by unexpected shutdown or illegal sequence

have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Dependencies: ADV_SPM.1 Informal TOE security policy model

(42). FPT_TST.1 TSF testing

Hierarchical to: No other components.

FPT_TST.1.1 The TSF shall run a suite of self tests during start-up to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide SBJ.STROM_A and SBJ.XAICAPF with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide SBJ.STROM_A and SBJ.XAICAPF with the capability to verify the integrity of stored TSF executable code.

Dependencies: FPT_AMT.1 Abstract machine testing

5.2.3. Applicable to TSFs of ST19XR34

(43). FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of events resulting from:

- Operating changes by the environment like:
  - Violation of physical integrity
  - Low/High voltage supply
  - High/Low frequency
- Access control violation attempts
- Bad EEPROM or CPU usage

known to indicate a potential security violation;

b) Make these indications available to SBJ.XAICAPF after a warm reset..

Application note:

As for FAU_SAA.1.1, some of TSFs are able to detect s potential attacks and record it on a register as an audit data. As for FAU_SAA.1.2, it is noticed that only cold reset is available in contactless mode.

Dependencies: FAU_GEN.1 Audit data generation

(44). FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 [JUKI]

FDP_ACC.2.1 The TSF shall enforce the SFP.CHIP on subjects and objects listed below and all operations among subjects and objects covered by the SFP.CHIP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.CHIP.

List of Subjects related to FDP_ACC.2

SBJ.STROM_A
SBJ.LIB_A
SBJ.ROMA_A
SBJ.EEPROMB_A
SBJ.EEPROMC_A

List of Objects related to FDP_ACC.2

OBJ.STROM_A
OBJ.ROMA_A
OBJ.RAMA_A
OBJ.RAMB_A
OBJ.RAMC_A
OBJ.RAMD_A
OBJ.EEPROM_A
OBJ.EEPAAB_A
OBJ.USERREGISTER_A
OBJ.STREGISTER_A

List of operations related to FDP_ACC.2

[ROM]: OP.READ_A
[RAM, REGISTER]: OP.READ_A, OP.WRITE_A
[EEPROM, EEPAAB]: OP.READ_A, OP.PROGRAM_A, OP.ERASE_A

Dependencies: FDP_ACF.1 Security attribute based access control

(45). FDP_ACF.1 [CHIP] Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the SFP.CHIP to objects based on SA.LOCATION_A or SA.EEPAAB_A.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed as follows

Table 5-w: SFP.CHIP related access matrix

<< The table is removed >>

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the none.

Dependencies: FDP_ACC.1 [JUKI] Subset access control,
FMT_MSA.3 Static attribute initialisation

(46). FDP_IFF.3 Limited illicit information flows

Hierarchical to: No other components.

FDP_IFF.3.1 The TSF shall enforce the SFP.DES to limit the capacity of electrical power consumption and electromagnetic emanation variations to an SPA, DPA, EMA and HODPA SOF high resistance level.

Dependencies: AVA_CCA.1 Covert channel analysis,
FDP_IFC.1 Subset information flow control

(47). FDP_IFF.4 Partial elimination of illicit information flows

Hierarchical to: FDP_IFF.3

FDP_IFF.4.1 The TSF shall enforce the SFP.RSA to limit the capacity of electrical power consumption and electromagnetic emanations variations to a SPA and EMA SOF high resistance level.

FDP_IFF.4.2 The TSF shall prevent electrical power consumption variations revealing SFP.RSA controlled information thereby being DPA and HODPA proof.

Dependencies: AVA_CCA.1 Covert channel analysis,
FDP_IFC.1 Subset information flow control

(48). FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the SFP.CHIP to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies:
[FDP_ACC.1 [JUKI] Subset access control, or FDP_IFC.1 Subset information flow control]

(49). FDP_RIP.1[CHIP] Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1[CHIP].1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects: OBJ.RAM*_A, OBJ.USERREGISTER_A and OBJ.STREGISTER but the illegal condition register and the CRC control register when in warm reset

Dependencies: No dependencies

(50). FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for following integrity errors;

- single bit fails upon a read operation on each byte

in OBJ.EEPROM_A on all objects, based on the following attributes: redundancy data.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall

- correct on the fly single bit fails on a read operation on each byte and report to the SF_ADMINIS_A ,
- report that all bits are set to one in a byte and its redundancy data upon a read operation to the SF_ADMINIS_A
- report that two bits fails on a read operation on each byte to the SF_ADMINIS_A.

Dependencies: No dependencies

Application note:

In this security statement, the ‘redundancy data’ means error checking code (ECC) of EEPROM.

(51). FMT_MSA.1 [CHIP] Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the SFP.CHIP to restrict the ability to change_default the security attributes SA.EEPAAB_A to ROL.CARDMAN and ROL.ISSUER1

Dependencies: [FDP_ACC.1 [JUKI] Subset access control or
FDP_IFC.1 Subset information flow control],
FMT_SMR.1 Security roles

(52). FMT_MSA.3 [CHIP] Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the SFP.CHIP to provide following default values for security attributes that are used to enforce the SFP.CHIP.

FMT_MSA.3.2 The TSF shall allow the following roles to specify alternative initial values to override the default values when an object or information is created.

Table 5-x: Authorized roles allowed to change default value of security attribute

Security Attribute	Default value	Role allowed to change
SA.LOCATION_A	Details not given for confidentiality reason	none
SA.EEPAAB_A	Details not given for confidentiality reason	ROL.CARDMAN ROL.ISSUER1

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

(53). FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For the clock and voltage supply operating changes by the environment like High/low voltage attack or High/low frequency attack, the TSF shall monitor the devices and elements and notify SBJ.XAICAPF when physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies: **FMT_MOF.1 Management of security functions behaviour**

(54). FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist operating changes by the environment, and physical integrity tampering like:

Violation of physical integrity

High/Low voltage attack

High/Low frequency attack

to the clock, voltage supply and shield layers by responding automatically such that the TSP is not violated.

Dependencies: No dependencies

(55). FPR_UNO.1 Unobservability

Hierarchical to: No other components.

FPR_UNO.1.1 The TSF shall ensure that all end-users are unable to observe the following operations on the following objects by SBJ.STROM_A and SBJ.LIB_A.

Table 5-y: List of unobserved operation among subjects and objects

operation	Objects on which operation can be performed by any subject
OP.READ_A	OBJ.STROM_A, OBJ.ROMA_A, OBJ.RAMA_A, OBJ.RAMB_A, OBJ.RAMC_A, OBJ.RAMD_A, OBJ.EEPROM_A, OBJ.EEPAAB_A, OBJ.USERREGISTER_A, OBJ.STREGISTER_A,
OP.WRITE_A	OBJ.RAMA_A, OBJ.RAMB_A, OBJ.RAMC_A, OBJ.RAMD_A,
OP.PROGRAM_A	OBJ.EEPROM_A, OBJ.EEPAAB_A
OP.ERASE_A	OBJ.EEPROM_A that indicates ‘ER0’ in SA.EEPAAB_A

Dependencies: No dependencies

5.3. Security functional requirements for IT environment

This section identifies security functional requirements for IT environment.

(56).FDP_RIP.1[ENV] Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from following objects: OBJ.TSF_*.

Dependencies: No dependencies

(57).FDP_ACC.1 [ENV] Subset access control

FDP_ACC.1.1 The TSF shall enforce the SFP.ENV

Subject	Issue program	
	Service program	
	Maintenance program	
Object	Smartcard (TOE)	
	Secret key of local government	
	Public key of JUKI authority	
	Terminal configuration data	
Operation	For TOE	Insert, Eject, Communicate
	For secret key	Store, Sign
	For public key	Store, Verify
	For terminal configuration data	Store, Change

Dependencies: FDP_ACF.1 Security attribute based access control

(58).FDP_ACF.1[ENV] Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the SFP.ENV to objects based on authentication records.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:.

Subject	Object	Operation to be allowed
Issue program	Smartcard (TOE)	Insert, Eject, Communicate
	Secret key of local government	Store
	Public key of JUKI authority	Store
Service program	Smartcard (TOE)	Insert, Eject, Communicate
	Secret key of local government	Sign
	Public key of JUKI authority	Verify
Maintenance program	Terminal configuration data	Store, Change

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules: none.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

(59). FMT_MSA.1[ENV] Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the SFP.ENV to restrict the ability to the security attributes to terminal administrator.

Dependencies: [FDP_ACC.1 [JUKI] Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

(60). FMT_MSA.3 [EMV] Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the SFP.ENV to provide restrictive default values for security attributes that are used TOE enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the issue operator to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

(61). FMT_SMR.1 [ENV] Security roles

FMT_SMR.1.1 The TSF shall maintain the following roles.

Terminal administrator

Issue operator

Service operator

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

(62). FIA_UID.1[ENV] Timing of identification

FIA_UID.1.1 The TSF shall allow password input request on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.4. Dependencies

This section shows all required dependencies in each security requirement and its assigned dependencies in Table 5-z.

Table 5-z: Dependencies

No.	SFRs of Xaica-PF	Required dependencies	Assignment
1	FAU_CFG.1	none	-
2	FCS_CKM.1[SMKEY]	FCS_CKM.2 or FCS_COP.1	FCS_CKM.2[SMKEY] FCS_COP.1
		FCS_CKM.4	FCS_CKM.4[SMKEY]
		FMT_MSA.2	unsupportive
3	FCS_CKM.1[RSAKEY]	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
		FCS_CKM.4	FCS_CKM.4[SMKEY]
		FMT_MSA.2	unsupportive
4	FCS_CKM.2[SMKEY]	FDP_ITC.1 or FCS_CKM.1	FDP_ITC.1[SMKEY] FCS_CKM.1[SMKEY]
		FCS_CKM.4	FCS_CKM.4[SMKEY]
		FMT_MSA.2	unsupportive
5	FCS_CKM.2[TMPKEY]	FDP_ITC.1 or FCS_CKM.1	FDP_ITC.2[TMKEY]
		FCS_CKM.4	FCS_CKM.4[TMPKEY]
		FMT_MSA.2	unsupportive
6	FCS_CKM.4[SMKEY]	FDP_ITC.1 or FCS_CKM.1	FDP_ITC.1[SMKEY] FCS_CKM.1[SMKEY]
		FMT_MSA.2	unsupportive
7	FCS_CKM.4[TMPKEY]	FDP_ITC.1 or FCS_CKM.1	FDP_ITC.2[TMKEY]
		FMT_MSA.2	unsupportive
8	FDP_ACC.1 [JUKI]	FDP_ACF.1	FDP_ACF.1[JUKI]
9	FDP_ACF.1 [JUKI]	FDP_ACC.1	FDP_ACC.1 [JUKI]
		FMT_MSA.3	FMT_MSA.3[JUKI]

			FMT_MSA.3[MODE]
10	FDP_ITC.1[DLO]	FDP_ACC.1or FDP_IFC.1	FDP_ACC.1 [JUKI]
		FMT_MSA.3	unsupportive
11	FDP_ITC.1[JUKI]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 [JUKI]
		FMT_MSA.3	FMT_MSA.3[JUKI]
12	FDP_ITC.1[SMKEY]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 [JUKI]
		FMT_MSA.3	unsupportive
13	FDP_ITC.2[DLO]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 [JUKI]
		[FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1
		FPT_TDC.1	FPT_TDC.1
14	FDP_ITC.2[TMPKEY]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 [JUKI]
		[FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1
		FPT_TDC.1	FPT_TDC.1
15	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
16	FIA_ATD.1	none	-
17	FIA_UAU.1	FIA_UID.1	FIA_UID.1
18	FIA_UAU.4	none	-
19	FIA_UAU.5	none	-
20	FIA_UAU.6	none	-
21	FIA_UID.1	none	-
22	FMT_MOF.1 [JUKI]	FMT_SMR.1	FMT_SMR.1
23	FMT_MOF.1[SE]	FMT_SMR.1	FMT_SMR.1
24	FMT_MSA.1 [JUKI]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 [JUKI]
		FMT_SMR.1	FMT_SMR.1
25	FMT_MSA.1 [MODE]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 [JUKI]

		FMT_SMR.1	FMT_SMR.1
26	FMT_MSA.3 [JUKI]	FMT_MSA.1	FMT_MSA.1[JUKI]
		FMT_SMR.1	FMT_SMR.1
27	FMT_MSA.3 [MODE]	FMT_MSA.1	FMT_MSA.1[MODE]
		FMT_SMR.1	FMT_SMR.1
28	FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
29	FMT_SMR.1	FIA_UID.1	FIA_UID.1
31	FTP_ITC.1	none	-
32	FPT_TDC.1	none	-
No	**Composite SFRs**	**Requireddependencies**	**Assignment**
33	FCS_COP.1	FDP_ITC.1 or FCS_CKM.1	FDP_ITC.1[SMKEY] FCS_CKM.1[SMKEY]
		FCS_CKM.4	FCS_CKM.4[SMKEY]
		FMT_MSA.2	unsupportive
34	FDP_IFC.1[DES]	FDP_IFF.1	FDP_IFF.1[DES]
35	FDP_IFC.1[RSA]	FDP_IFF.1	FDP_IFF.1[RSA]
36	FDP_IFF.1[DES]	FDP_IFC.1	FDP_IFC.1[DES]
		FMT_MSA.3	unsupportive
37	FDP_IFF.1[RSA]	FDP_IFC.1	FDP_IFC.1[RSA]
		FMT_MSA.3	unsupportive
38	FIA_SOS.2	none	-
39	FPT_FLS.1	ADV_SPM.1	ADV_SPM.1
40	FPT_RCV.2	FPT_TST.1	FPT_TST.1
		AGD_ADM.1	AGD_ADM.1
		ADV_SPM.1	ADV_SPM.1
41	FPT_RCV.4	ADV_SPM.1	ADV_SPM.1
42	FPT_TST.1	FPT_AMT.1	unsupportive
No	**SFRs on ST19XR34**	**Required dependencies**	**Assignment**
30	FPT_SEP.1	none	none
43	FAU_SAA.1	FAU_GEN.1	unsupportive
44	FDP_ACC.2	FDP_ACF.1	FDP_ACF.1 [CHIP]
45	FDP_ACF.1[CHIP]	FDP_ACC.1	FDP_ACC.2
		FMT_MSA.3	FMT_MSA.3 [CHIP]
46	FDP_IFF.3	AVA_CCA.1	unsupportive

		FDP_IFC.1	FDP_IFC.1 [DES]
47	FDP_IFF.4	AVA_CCA.1	unsupportive
		FDP_IFC.1	FDP_IFC.1 [RSA]
48	FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.2
49	FDP_RIP.1[CHIP]	none	-
50	FDP_SDI.2	none	-
51	FMT_MSA.1 [CHIP]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.2
		FMT_SMR.1	FMT_SMR.1
52	FMT_MSA.3[CHIP]	FMT_MSA.1	FMT_MSA.1[CHIP]
		FMT_SMR.1	FMT_SMR.1
53	FPT_PHP.2	FMT_MOF.1	unsupportive
54	FPT_PHP.3	none	-
55	FPR_UNO.1	none	-
No	**SFRs on IT environment**	**Required dependencies**	**Assignment**
56	FDP_ACC.1 [ENV]	FDP_ACF.1	FDP_ACF.1[ENV]
57	FDP_ACF.1 [EMV]	FDP_ACC.1	FDP_ACC.1 [ENV]
		FMT_MSA.3	FMT_MSA.3[ENV]
58	FMT_MSA.1 [EMV]	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1
		FMT_SMR.1	FMT_SMR.1 ENV
59	FMT_MSA.3 [EMV]	FMT_MSA.1	FMT_MSA.1[ENV]
60	FMT_SMR.1 [EMV]	FIA_UID.1	FIA_UID.1 ENV
61	FIA_UID.1 [EMV]		

5.5. Minimum strength of function claim

The minimum strength of TOE function is claimed as SOF-high.

6. TOE security assurance requirements

This chapter describes the TOE security assurance requirements.

In this security target, EAL4 augmented with ADV_IMP.2 and ALC_DVS.2 is required as security assurance.

Table 6-a: TOE security assurance class and components

Assurance class	Assurance requirement component
ASE: Security Target evaluation	ASE_INT.1 ASE_DES.1 ASE_ENV.1 ASE_OBJ.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1 ASE_PPC.1
ACM: Configuration management	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO: Delivery and operation	ADO_DEL.2 ADO_IGS.1
ADV: Development	ADV_FSP.2 ADV_HLD.2 ADV_IMP.2 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1

AGD: Guidance documents	AGD_ADM.1 AGD_USR.1
ALC: Lifecycle support	ALC_DVS.2 ALC_LCD.1 ALC_TAT.1
ATE: Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA: Vulnerability assessment	AVA_MSU.2 AVA_SOF.1 AVA_VLA.2

7. TOE summary specification

This chapter presents the overview specification of TOE functions.

7.1. Lifecycle

This section refines the environment, management and deliveries between entities in each phases of lifecycle, according to [PP9806].

- Phase 1	Smartcard embedded software development phase
- Phase 2	IC chip development
- Phase 3	IC chip manufacturing and testing
- Phase 4	IC chip packaging and testing
- Phase 5	Smartcard product finishing process
- Phase 6	Smartcard personalization
- Phase 7	Smartcard end-usage

7.1.1. Phase 1 Smartcard embedded Software development phase

NTTDATA is a sponsor and the embedded software (ES) developer, responsible for the ES design specification, quality of ES functionalities implemented in ES (Xaica-PF). TOPPAN is a supportive developer, in charge of coding of the program.

7.1.2. Phase 2 IC chip development

STM is responsible for determining IC chip specification and the design of circuit, programs, and verifies all the functions on it.

Delivery among Phase1 and Phase2

Following items are delivered in order to require STM to product customized IC chip.

- Software program embedded on IC chip (Xaica-PF)
- Requirement of mask

7.1.3. Phase 3&4 IC chip production, packaging and testing

STM is responsible for IC chip production, packaging and testing. IC chip is customized with requirement for mask and Xaica-PF program delivered from ES developer. Note that Phase 4 (IC packaging and testing) is out of evaluation scope.

Delivery between Phase4 and Phase5

IC chip module of ST19XR34 is delivered from STM to card manufacturer after the production process in Phase4 is completed successfully.

<<The figure is removed>>

Figure 7-1: Lifecycle of the TOE

7.1.4. Phase 5 Smartcard finishing process

Phase5 covers 'initial', 'manufacturing' or 'pre-production' of card-status .

'initial'

After card manufacturer received IC module, the smartcard Xaica-alpha (TOE) is produced through the card manufacturing process (PHASE5) as the status of card lifecycle is 'initial'. In this phase, some of basic files are created as like CD, system track, and so on.

'manufacturing'

In 'manufacturing phase, TOE can be activated only by ROL.CARDMAN (in case SA.S_MODE = 'normal') or ROL.TEST (in case of SA.S_MODE = 'test')

Two keys for ROL.ISSUER1 and ROL.ISSUER2 shall be created in this phase.

'pre-production'

In 'initialization' phase, TOE can be activated only by ROL.ISSUER1 .

Delivery between Phase5 to Phase6

TOE is delivered from card manufacturer to card issuer .

7.1.5. Phase 6 Smartcard personalization

Phase6 covers ‘initialization’, ‘Password-setting’ of card-status.

‘initialization’

In ‘initialization’ phase, TOE can be activated only by ROL.ISSUER2 . SD and RDF for applications are downloaded with userdata and keys .

‘Password-setting

This phase is used only for JUKI-application , in order to set or change user password.

7.1.6. Phase 7 Smartcard end-usage

Phase 7 covers ‘CD-secured’, ‘CD-locked, ‘CD-terminated’ of card-status

‘CD-secured’

In ‘CD-secured’, card user can use TOE in the smartcard services. .

‘CD-locked’

In ‘CD-locked, TOE is locked so that only restricted actions can be allowed by user, and only an authorized user can change the Card-status to ‘CD-secured’.

‘CD-terminated’

TOE stops all the functionality in this phase.

<<The figure is removed>>

Figure 7-2: Card-status and corresponding lifecycle phases

7.2. Basic IT functions

7.2.1. Command and response

TOE has the contact interface as well as the contactless interface. Contact interface supports T=1 protocol as TPDU, and also contactless interface supports

ISO/IEC14443 type B as TPDU.

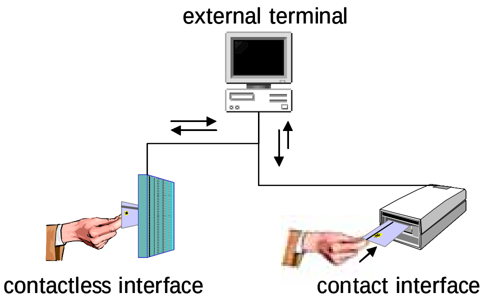

Figure 7-3: Dual interface

After initialization and initial testing are finished, Xaica-PF waits for receiving external command sent from external terminal as shown in Figure 7-4. When external command is received, TOE processes the command function as required in external command, and TOE sends the response to external terminal.

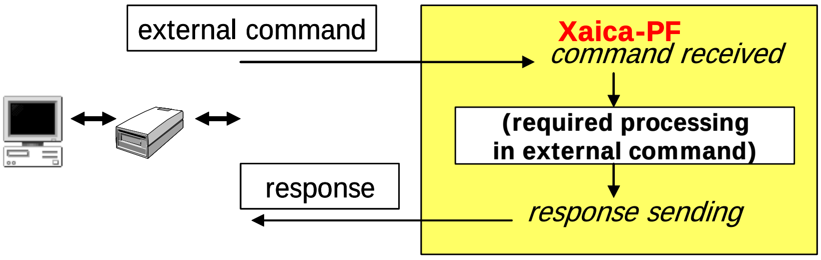

Figure 7-4: Command and response

7.2.2. Domain and file management

TOE has one logical domain named **Card Domain (CD)** for card management, and it has also the function to manage the files, service domains or **smartcard applications**. It is possible to create the **IEF (Internal Elementary File)** or **WEF (Working Elementary File)** under CD. IEF means the file which holds PIN or cryptographic keys. WEF means the file which holds any service data. And also it can be allowed to download **Service Domain (SD)** on CD. It is also possible to create the IEF, WEF, and smartcard application under SD. SD can be downloaded with or without verification of its signature. Security attributes on CD determines whether the verification of SD's signature is needed or not.

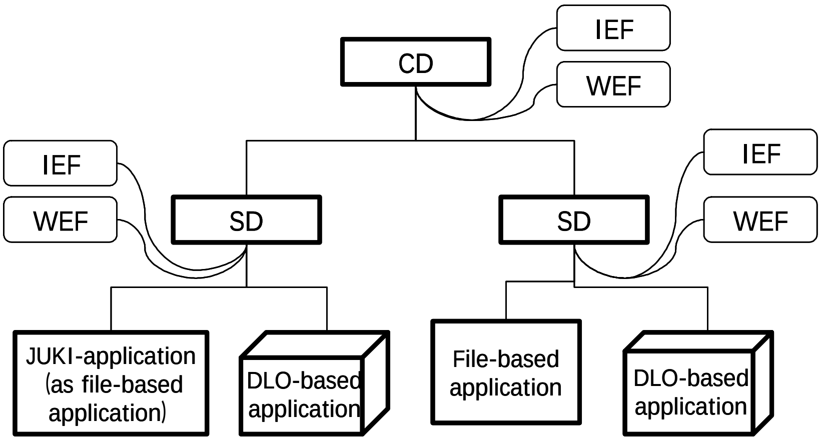

Figure 7-5: Structure of files and domains

7.2.3. Application identification

Usually the user selects the application by SELECT command with **AID (Application ID)**. AID uniquely identifies the smartcard application. TOE can identify the application by AID in SELECT command.

<< The figure is removed >>

Figure 7-6: Application identification

7.2.4. Application management

File-based application has one RDF (Root DF) as a top level directory of application and **DF (Dedicated File)**, WEF or IEF. It is also possible to create IEF or WEF (or DF) under DF.

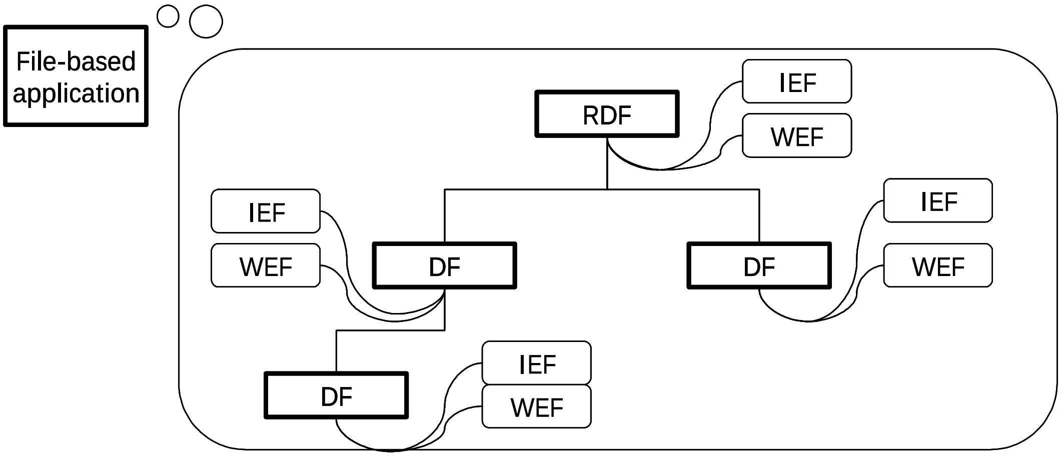

Figure 7-7: Structure of file-based application

7.2.5. Memory partition and access control

Memories on ST19XR34 are partitioned as **ST-ROM**, **ROM-A** as a Read Only Memory, **EEPROM-A,B,C** as a Non Volatile Memory and **RAM-A,B** as a Volatile Memory. Any data, keys or programs can be stored, managed or executed on one of them.

ST19XR34 provides the functionality to manage the access control of process accessing the memory according to security attribute.

<< The figure is removed >>

Figure 7-8 : Access matrix

<< The figure is removed >>

Figure 7-9 : Access control

7.3. TOE security functions

There are two types of TOE security functions (TSFs); one is provided by Xaica-PF and the other is provided by ST19XR34.

Table 7-a: TOE security functions

1) TSFs provided by Xaica-PF

No.	Symbol	Name of TSF
1	SF_I&A	Identification and authentication
2	SF_ACCESS	Access control
3	SF_CRYPTO	Cryptography
4	SF_LIFECYCLE	Management of Card-status
5	SF_SM	Secure messaging
6	SF_SMKEY	Management of secure messaging key(s)
7	SF_KEYPW	Management of keys and password
8	SF_TMPKEY	Management of temporary public key
9	SF_DOWNLOAD	Download
10	SF_SE	Management of SE
11	SF_INITIALTEST	Initial testing

2) TSFs provided by ST19XR34

	Symbol	Name of TSF
12	SF_CONFIG_A	TOE configuration switching and control
13	SF_INIT_A	Hardware initialisation & TOE attribute initialization
14	SF_INT_A	IC logical integrity
15	SF_FWL_A	Storage and Function access firewall
16	SF_PHT_A	Physical tampering security function
17	SF_ADMINIS_A	Security violation administrator
18	SF_OBS_A	Unobservability
19	SF_SKCS_A	Symmetric key cryptography support
20	SF_AKCS_A	Asymmetric key cryptography support
21	SF_ALEAS_A	Unpredictable number generation support

7.3.1. TSFs provided by Xaica-PF

(1)SF_I&A: Identification and authentication

SF_I&A provides the function to authenticate and identify the user Any user shall require the authentication to the TOE with **key-ID**. If authentication is succeeded TOE identifies the authorized user as key-ID by writing authorized user (key-ID) on the temporary data area internally (it is called '**security status**').

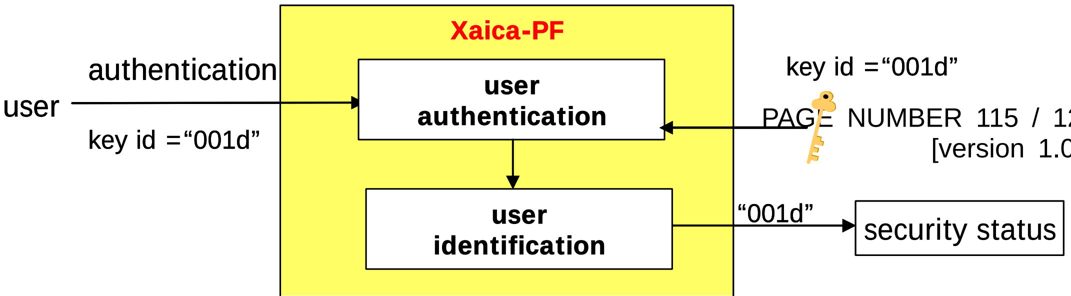

Figure 7-10: User identification and authentication

Authentication mechanism provides:

- PIN-verification (‘VERIFY’ command)
- Dynamic authentication (‘EXTERNAL AUTHENTICATE’ command)
- Static authentication (‘VERIFY DIGITAL SIGNATURE’ command)
- Dynamic / Static authentication with temporary public key.

(2)SF_ACCESS: Access control

SF_ACCESS has the responsibility to allow only authorized user to access object in the TOE, with referring to security status, card-status and security attributes associated to the object.

(3)SF_CRYPTO: Cryptographic function

SF_CRYPTO provides following cryptographic functions:

- T-DES2key … Triple DES using 2 keys, which is standard T-DES.
- T-DES3key … Triple DES using 3 keys, supported as required in JUKI-service.
- RSA … Asymmetric cryptography, as required in JUKI-service.

These are used for encryption, decryption, secure messaging, authentication, computing signature, verification of signature or certificate.

(4)SF_LIFECYCLE: Management of Card-status

SF_LIFECYCLE manages the status of TOE itself (**card-status**), each of which is applicable from initial issuing to termination. Only authorized users are allowed to change card-status.

<< The figure is removed >>

Figure 7-11: Card-status management

<< The figure is removed >>

Figure 7-12: Lifecycle and card-status

(5)SF_SM: Secure messaging

In order to keep confidentiality and integrity of external command and response between TOE and external terminal, SF_SM provides functions to establish secure communication (**secure messaging**), which covers:

- Encryption and decryption of external command and response
- Computation and verification of message authentication code (MAC)

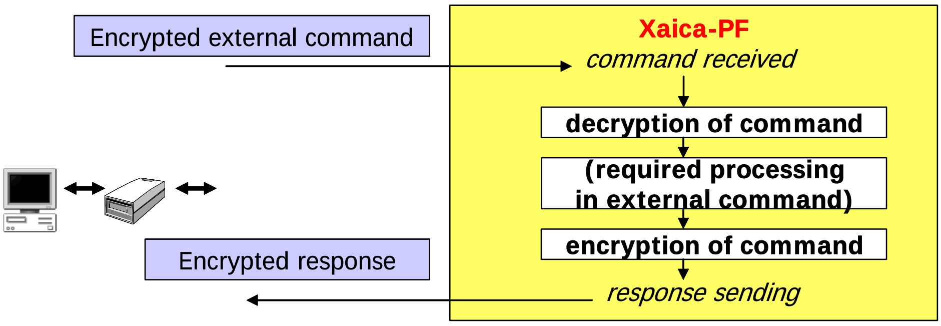

Figure 7-13: Secure Messaging

(6)SF_SMKEY: Management of secure messaging keys

As TOE is required to share the key(s) with external terminal before secure messaging is established, SF_SMKEY gives the functionality of key distribution mechanism and to manage the secure messaging key(s) after distributed.

(7)SF_KEYPW: Management of keys and password

SF_KEYPW provides key and/or password management function for roles.

Table 7-b: State transition and management of password

<< The table is removed >>

(8)SF_TMPKEY: Management of temporary public key

By using SF_TMPKEY, RSA public key can be downloaded to be kept available temporarily (temporary public key) after successful verification of certificate. Such a temporary public key can be used for authentication.

(9)SF_DOWNLOAD: Management of Smartcard application downloading

SF_DOWNLOAD provides the function of secure downloading of.

- SD with WEFs and/or IEFs
- File-based application including RDF with WEF and/or IEFs

. If necessary, SF_DOWNLOAD performs verification of signature assigned with objects. This function also allows user to delete downloaded objects.

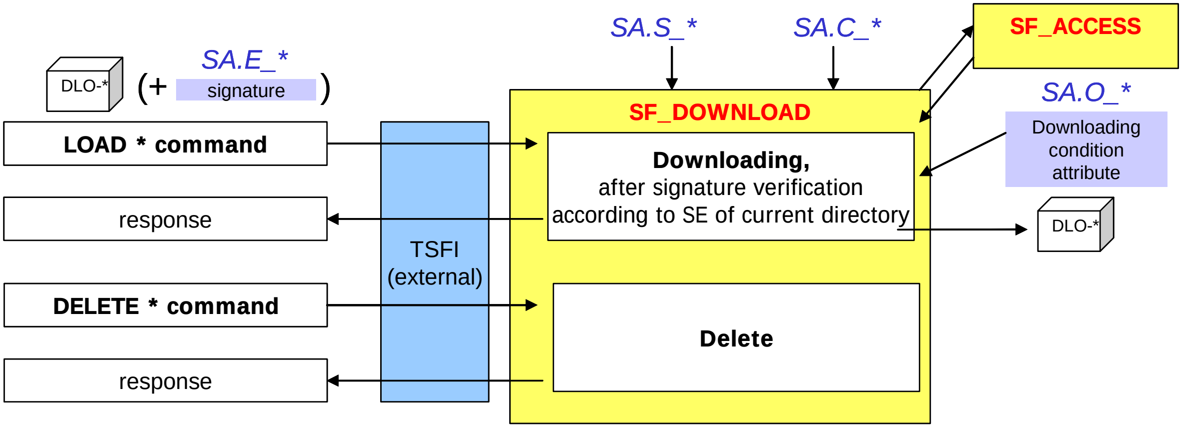

Figure 7-14: Download function

(10)SF_SE: Management of SECURITY ENVIRONMENT

SF_SE provides management function of SECURITY ENVIRONMENT as defined in [ISO7816], which enables to manage security attributes covering:

· Method of secure messaging key distribution

· Cryptographic algorithm used in secure messaging

· Keys used for signature computation or verification of signature, and so on.

SECURITY ENVIRONMENT is basically managed only by authorized user, which also depends on the security attributes of CD, SD, RDF or DF.

(11) SF_INITIALTEST: Initial testing of TOE

When **Power-on** or **warm reset** is performed, TOE performs **the hardware and TOE attributes initialization** (internal variables, registers clear and so on) and **initial testing** in SF_INITIALTEST in order to make TOE itself initialized ,as well as to recover data, key or program integrity and analyze the fault or violation of the previous session.

<< The figure is removed >>

Figure 7-15: Initial testing function

7.3.2. TSFs provided by ST19XR34

(12)SF_CONFIG_A : CHIP configuration switching and control

SF_CONFIG_A handles three configurations of TEST, ISSUER and USER as '**Chip configuration**'. However, in this security target, it is assumed that only USER configuration is available, which allows embedded software to execute any authorized actions after the end of PHASE 4.

(13) SF_INIT_A: Hardware initialisation & TOE attribute initialisation

SF_INIT_A starts initially when the power-on or warm reset is done, which supports SF_INITIALTEST.

(14)SF_INT_A: IC logical integrity

This functionality is responsible for following operations,

- valid CPU usage and stack overflow verification
- for correcting single bit fails upon a read operation
- other actions not described [ST19XR34-ST]

(15)SF_FWL_A: Storage and Function Access Firewall

SF_FWL_A is responsible for preserving correct access and operations of subject, monitoring access, and notification of access violation attempts to SF_ADMINIS_A.

(16)SF_PHT_A: Physical tampering security function

SF_PHT_A is responsible for detecting environmental changes or attempts to violate its physical integrity, reporting them to SF_ADMINIS_A.

(17)SF_ADMINIS_A: Security violation administrator

This functionality ensures the management of security violations attempts, reported by other TSFs.

Upon detection of a security violation attempt, this functionality is responsible for the interrupt vectors management and for the TOE automatic response generation, if any.

(18)SF_OBS_A: Unobservability

SF_OBS_A provides security functionalities relating not only IT countermeasures like internal data transfer encryption, clock configuration but also the material countermeasures like physical integrity detectors.

(19)SF_SKCS_A: Symmetric Key Cryptography Support

SF_SKCS_A provides symmetric key cryptographic functionalities (T-DES), which supports SF_CRYPTO.

(20)SF_AKCS_A: Asymmetric Key Cryptography Support

SF_AKCS_A provides asymmetric key cryptographic functionalities (RSA), which supports SF_CRYPTO.

(21)SF_ALEAS_A: Unpredictable Number Generation Support

SF_ALEAS_A provides unpredictable number generation functionalities, which complies NIST FIPS PUB-140-2:1999 standard for a Security Level 3 cryptographic module (statistical test upon demand)

7.4. Analysis of strength of functions

Following TSFs are related to the probabilistic or permutational function. Only one TOE security function is related to probabilistic or permutational.

- SF_I&A as ‘high’ level of SOF.

SF_I&A has cryptographic authentication with following features:

- Limitation of allowed authentication failure could be set as 3.

SF_I&A has also PIN-verification mechanism with following features:

- Limitation of allowed authentication failure could be set as 3.
- Digits of PIN from 4 up to 16

Above implementation is recommended in the guidance documentation, and also it is recommended that the locked key or PIN should not be unlocked without the authorized role's permission. Therefore, the strength of function analysis could reach the conclusion that TOE meets 'SOF-high'.

Note that following TSFs are out of scope for strength of functions analysis because these are related to the cryptographic or random generation mechanism

- SF_CRYPTO
- SF_AKCS_A
- SF_SKCS_A
- SF_ALEAS_A

7.5. Assurance measures

This section provides a list of documents delivered as assurance measures, all of which are claimed to satisfy the stated assurance requirements.

Table 7-c: Assurance measures

Class	Component	Assurance measure
ASE	ASE_*	Xaica-alpha - Security target [ver1.02]
ADV	ADV_FSP.2	Xaica-alpha - Functional specification [ver1.00] Xaica-alpha - Platform specification [ver1.00] Xaica-alpha - Interface Matrix [ver1.00] Xaica-Alpha - Security Specification [ver1.02] Xaica-alpha - Low Layer Specification [ver1.06]
	ADV_RCR.1	Xaica-alpha - Traceability analysis (ST-FS)
	ADV_HLD.2	Xaica-alpha - High Level Design [ver1.01]
	ADV_RCR.1	Xaica-alpha - Traceability analysis (FS-HLD)
	ADV_LLD.1	Xaica-alpha - Low Level Design [ver1.01]
	ADV_RCR.1	Xaica-alpha - Traceability analysis (HLD-LLD)
	ADV_IMP.2	alpha7r, alphacpt7r_E, AesLib7r, Alphacpt7r, ansicb,

		rf_Alpha7r, RSALIB7r
	ADV_RCR.1	Xaica-alpha - Traceability analysis (LLD-IMP)
	ADV_SPM.1	Xaica-alpha - TOE security policy model
ATE	ATE_COV.2, ATE_DPT.2, ATE_FUN.1	Xaica-alpha - Test analysis [ver1.02] Xaica-alpha - Test documentation [ver1.02] Xaica-alpha - Test report [ver1.02]
	ATE_IND.2	Xaica-alpha - Development tool - manual for Scenario Drawer Xaica-alpha - Development tool - manual for Scenario Simulator Xaica-alpha - Development tool - set-up manual for development tools (TOOL) Scenario Drawer - English version (TOOL) Scenario Simulator - English version
		(CARD) Sample cards of TOE
AVA	AVA_SOF.1	Xaica-alpha - Analysis for strength of function
	AVA_VLA.2	Xaica-alpha - Vulnerability analysis [ver1.01]
	AVA_MSU.2	Xaica-alpha - Guidance analysis
AGD	AGD_ADM.1	Xaica-alpha - Guidance for card issuer
	AGD_USR.1	Xaica-alpha - Guidance for service provider Xaica-alpha - Guidance for card holder Guidance for Service Provider [Command APDU Specifications] Security manual for developer [ver1.02]
ACM ALC	ACM_CAP.4 ACM_SCP.2 ACM_AUT.1	Xaica-alpha - Summary of project security [ver1.02] Xaica-alpha – Configuration Management System ALPHA-NTTD-PRJ-CMN_J ALPHA-NTTD-PRJ-VER150i_alpha7rs3_SM032 SDDCOP-CFM-020- Configuration Management System ALPPUO-PMN-020-Project Control Document ALPPUO-VER-010-Version Management Document ALPCOP-CDM-020-Code Management Document ALPCOP-DLR-020-Rom Code Distribution Procedures ALPCOP-GNT-020-Rom Code Generation Procedures ALPCOP-SMM-060-Softmask Management Document

	ALC_DVS.2 **ALC_LCD.1**	**Xaica-alpha - Summary of project security [ver1.02]** **SDDCOP-DVL-020- Security In The Development Environment** **ALPCOP-LCD-030-Lifecycle Definition Document**
	ALC_TAT.1	**Xaica-alpha - Manual for Scenario Drawer**
		Xaica-alpha - Manual for Scenario Simulator
		Xaica-alpha - Set-up manual for development tools
		Code warrior tool manual
ADO	**ADO_DEL.2** **ADO_IGS.1**	**Xaica-alpha - Guidance for card issuer** **ALPCOP-IGS - Card Issue Process For Card Manufacturers** **ALPCOP-IG3 - Installation guidance for 3rd vendor**

8. PP claims

This section is omitted because this security target does not comply with any Protection Profile.

9. Rationale

For confidentiality reasons, the rationale is not described here.

10. References

10.1. Common Criteria and ISO15408

- [ISO15408] ISO/IEC 15408 – Information Technology – Security Techniques – Evaluation Criteria for IT Security
- [CC_Part1] Common Criteria Security Evaluation Part 1: Introduction and general model, August 1999,Version 2.1,CCIMB-99-031
- [CC_Part2] Common Criteria Security Evaluation Part 2: Security functional requirements, August 1999,Version 2.1,CCIMB-99-032
- [CC_Part3] Common Criteria Security Evaluation Part 3: Security assurance requirements, August 1999,Version 2.1,CCIMB-99-033
- [JIS5070] JIS X 5070 Security technologies - IT security evaluation criteria
- [JIS6300] JIS X 6300 IC card with logical interface
- [JIS6322] JIS X6322 Contactless IC card

10.2. PP, ST and ST19XR34 related documentations

- [PP9806] … Protection Profile Smartcard Integrated Circuit; Version 2.0, Sep 1998.
- [JUKI-PP] …THE RESIDENTIAL IC CARD PROTECTION PROFILE version1.5E, Local Authorities Systems Development Centre (LASDEC)
- [ST-ST19XR34] … Security Target Lite for ST19XR34,
  PID_GRENAT_ST_02_004_V01.20, STMicroelectronics
- [CertRepo-ST19XR34] … "Rapport de certification 2004/31, Micro-circuit ST19XR34F, EAL4 augmented", October 2004 issued by DCSSI.

10.3. JUKI-service related documents

- [JUKI-network] Overview of JUKI-network system <Japanese version>
- [JUKI-spec] Specification for JUKI-card ver2.1 <Japanese version>
- [JUKI-type2] Specification for JUKI-card type2 ver0.9 <Japanese version>

- [JUKI-test] Guidance for the testing of JUKI-card ver2.0 <Japanese version>

10.4. Smartcard standards

- [ISO7816] ISO/IEC 7816 - Identification Cards - Integrated Circuit Cards with Contacts
- [ISO14443] ISO/IEC 14443 - Contactless Integrated Circuit Cards, Proximity Cards
- [JICSAP] JICSAP (Japan IC Card System Application council) specification ver1.1